GFI MailEssentials™

Administratorhandbuch

Die Informationen in diesem Dokument dienen ausschließlich Informationszwecken und werden in der vorliegenden Form ohne (ausdrückliche oder stillschweigende) Haftung jeglicher Art bereitgestellt, insbesondere ohne Gewährleistung der Marktgängigkeit, der Eignung für einen bestimmten Zweck oder der Nichtverletzung von Rechten. GFI Software haftet nicht für etwaige Schäden, einschließlich Folgeschäden, die sich aus der Nutzung dieses Dokuments ergeben. Die Informationen stammen aus öffentlich zugänglichen Quellen. Trotz sorgfältiger Prüfung der Inhalte übernimmt GFI keine Haftung für die Vollständigkeit, Richtigkeit, Aktualität und Eignung der Daten. Des Weiteren ist GFI nicht für Druckfehler, veraltete Informationen und Fehler verantwortlich. GFI übernimmt keine Haftung (ausdrücklich oder stillschweigend) für die Richtigkeit oder Vollständigkeit der in diesem Dokument enthaltenen Informationen.

Nehmen Sie mit uns Kontakt auf, wenn Ihnen in diesem Dokument Sachfehler auffallen. Wir werden Ihre Hinweise sobald wie möglich berücksichtigen.

Windows, Exchange, IIS, .NET, Internet Explorer, Outlook, SQL Server und Microsoft sind Marken oder eingetragene Marken der Microsoft Corporation in den Vereinigten Staaten und anderen Ländern.

Alle hier aufgeführten Produkte und Firmennamen sind Marken der jeweiligen Eigentümer.

GFI MailEssentials unterliegt dem urheberrechtlichen Schutz von GFI SOFTWARE LTD. - 1999-2014GFI Software Ltd. Alle Rechte vorbehalten.

Dokumentenversion: 2.1.1

Zuletzt aktualisiert (Monat/Tag/Jahr): 3/3/2014

Inhaltsverzeichnis

1 Einführung **10**

1.1 Info zu diesem Handbuch 10
1.2 Begriffe und Konventionen dieses Handbuchs 11

2 Informationen zu GFI MailEssentials **12**

2.1 Komponenten von GFI MailEssentials 12
2.2 Filterung eingehender E-Mails 14
2.3 Filterung ausgehender E-Mails 14
2.4 Scan- und Filter-Engines für E-Mails 15
2.5 Typische Bereitstellungsszenarien 17
2.6 Endbenutzeraktionen 19

3 Installation **21**

3.1 Systemanforderungen 21
3.2 Aktionen vor der Installation 24
3.3 Installationsvorgang 39
3.4 Aktualisieren von früheren Versionen 47
3.5 Aktionen nach der Installation 49

4 Statusüberwachung **53**

4.1 Dashboard 53
4.2 Berichte 61

5 E-Mail-Sicherheit **73**

5.1 Virenscan-Engines 73
5.2 Informationsspeicherschutz 96
5.3 Scanner für Trojaner und ausführbare Dateien 99
5.4 E-Mail-Exploit-Engine 103
5.5 HTML-Bereinigung 107

6 Anti-Spam **111**

6.1 Anti-Spam-Filter 111
6.2 Spam-Aktionen – Umgang mit Spam-E-Mails 150
6.3 Sortieren der Anti-Spam-Filter nach Priorität 153
6.4 SMTP-Übertragungsfilterung 154
6.5 Spam-Bericht 156
6.6 Anti-Spam-Einstellungen 158
6.7 SpamTag für Microsoft Outlook 166
6.8 Scannen öffentlicher Ordner 174

7 Inhaltsfilterung **180**

7.1 Stichwortfilterung 180
7.2 Anhangsfilterung 187
7.3 Erweiterte Inhaltsfilterung 195
7.4 Dekomprimierungs-Engine 201

8 Quarantäne **208**

8.1 Wichtige Hinweise 208
8.2 Durchsuchen der Quarantäne 208
8.3 Suchordner 214
8.4 Arbeiten mit E-Mails in Quarantäne 217
8.5 Quarantäne-RSS-Feeds 221
8.6 Quarantäneoptionen 223
8.7 Speicherort des Quarantänespeichers und öffentliche URL 229

9 E-Mail-Verwaltung **232**

9.1 Haftungsausschlüsse 232
9.2 Automatische Antworten 236
9.3 Listenserver 238
9.4 E-Mail-Überwachung 243

10 Allgemeine Einstellungen **245**

10.1 Administrator-E-Mail-Adresse 245
10.2 Aktivieren/Deaktivieren von Scan-Modulen 245
10.3 Proxy-Einstellungen 246
10.4 Lokale Domänen 248
10.5 Verwalten lokaler Benutzer 249
10.6 Lizenzierung 250
10.7 Bindungen an virtuelle SMTP-Server 250
10.8 Patch-Überprüfung 250
10.9 Zugriffssteuerung 251

11 Verschiedene Themen **253**

11.1 Installationsinformationen 253
11.2 Namen der virtuellen Verzeichnisse 254
11.3 Benutzeroberflächenmodus 254
11.4 Fehlgeschlagene E-Mails 259
11.5 Rückverfolgung 260
11.6 POP2Exchange – E-Mails vom POP3-Server herunterladen 262
11.7 Verschieben von Spam-E-Mails in Benutzerpostfachordner 266
11.8 Verschieben von Spam in einen Exchange 2010-Ordner 268
11.9 Synchronisieren der Konfigurationsdaten 269
11.10 Deaktivieren der E-Mail-Verarbeitung 281
11.11 E-Mail-Sicherung vor und nach der Verarbeitung 282
11.12 Fernzugriffsports 283
11.13 Überwachen der Virus Scanning API 284

12 Fehlerbehebung und Support **289**

12.1 Einführung 289
12.2 Häufige Probleme 289
12.3 Scan-Engines und Filter 291
12.4 E-Mail-Verwaltung 292
12.5 GFI SkyNet 293

12.6 Webforum 293
12.7 Technischen Support anfragen 293
12.8 Dokumentation 293

13 Anhang – Bayes'scher Filter 294

14 Glossar 298

15 Index 305

Abbildungsverzeichnis

Screenshot 1: Prüfen des MX-Eintrags des DNS 32
Screenshot 2: Lotus Domino Administrator: Klicken auf die Option „Configurations“ („Konfigurationen“) ... 33
Screenshot 3: Klicken auf die Option „Edit Configuration“ („Konfiguration bearbeiten“) 33
Screenshot 4: LDAP-Einstellungen von Lotus Domino 34
Screenshot 5: Anonyme Authentifizierung aktivieren 35
Screenshot 6: Eine neue Datenbank anlegen 36
Screenshot 7: Konvertierungsergebnis laden 36
Screenshot 8: Einen Link zur aktuellen Anwendung in die Zwischenablage kopieren 37
Screenshot 9: Bei Anforderung einer Ordnerliste alle öffentlichen Ordner und Ordner anderer Benutzer einbeziehen 37
Screenshot 10: Neue Eingangs-E-Mail-Datenbank 38
Screenshot 11: Scannen öffentlicher Ordner aktivieren 39
Screenshot 12: Angabe der E-Mail-Adresse des Administrators und des Lizenzschlüssels 41
Screenshot 13: Informationen zum SMTP-Server und virtuellen Verzeichnis 42
Screenshot 14: DNS-Servereinstellungen 43
Screenshot 15: Proxy-Einstellungen 44
Screenshot 16: Domänen für eingehende E-Mails 44
Screenshot 17: SMTP-Servereinstellungen 45
Screenshot 18: Auswahl der standardmäßigen Anti-Spam-Aktion 46
Screenshot 19: Erstellen einer Testregel für die Stichwortfilterung 51
Screenshot 20: Durch Testregel blockierte Test-E-Mails 52
Screenshot 21: Das GFI MailEssentials Dashboard 54
Screenshot 22: Die GFI MailEssentials-Dienste 55
Screenshot 23: Quarantänestatistik 55
Screenshot 24: Dashboard-Diagramme 56
Screenshot 25: E-Mail-Verarbeitungsprotokolle 57
Screenshot 26: Filter für E-Mail-Verarbeitungsprotokolle 58
Screenshot 27: Aktualisierungen für Virenscan-Engines 59
Screenshot 28: Ereignisprotokolle 60
Screenshot 29: POP2Exchange-Protokoll 61
Screenshot 30: Erstellen eines Berichts 62
Screenshot 31: Diagrammbericht zu blockierten E-Mails 64
Screenshot 32: Durchsuchen der Berichtsdatenbank 67
Screenshot 33: Suchergebnisse aus der Berichtsdatenbank 68
Screenshot 34: Konfigurieren eines Microsoft® Access-Datenbank-Backends 69
Screenshot 35: Konfigurieren eines SQL Server-Datenbank-Backends 70
Screenshot 36: Konfiguration von Vipre 74
Screenshot 37: Aktionen der Virenscan-Engine 75
Screenshot 38: Aktualisierungen für Virenscan-Engines 76

Screenshot 39: Konfiguration von BitDefender 78
Screenshot 40: Aktionen der Virenscan-Engine 80
Screenshot 41: Aktualisierungen für Virenscan-Engines 81
Screenshot 42: Konfiguration von Kaspersky 83
Screenshot 43: Aktionen der Virenscan-Engine 84
Screenshot 44: Aktualisierungen für Virenscan-Engines 85
Screenshot 45: Konfiguration von Norman 87
Screenshot 46: Aktionen der Virenscan-Engine 89
Screenshot 47: Aktualisierungen für Virenscan-Engines 90
Screenshot 48: Konfiguration von McAfee 92
Screenshot 49: Aktionen der Virenscan-Engine 93
Screenshot 50: Aktualisierungen für Virenscan-Engines 95
Screenshot 51: Knoten für den Informationsspeicherschutz 97
Screenshot 52: VSAPI-Einstellungen 98
Screenshot 53: Scanner für Trojaner und ausführbare Dateien: Registerkarte 'Allgemein' 100
Screenshot 54: Aktualisierungen für Virenscan-Engines 102
Screenshot 55: Konfiguration der E-Mail-Exploit-Engine 103
Screenshot 56: Virenscan-Engine: Konfigurationsseite (Registerkarte für Aktionen) 104
Screenshot 57: Aktualisierungen für Virenscan-Engines 105
Screenshot 58: Liste der E-Mail-Exploits 107
Screenshot 59: Konfigurationsseite der HTML-Bereinigung 108
Screenshot 60: Whitelist-Seite der HTML-Bereinigung 109
Screenshot 61: Domänen-/IP-Ausschlüsse 110
Screenshot 62: Eigenschaften von SpamRazer 113
Screenshot 63: Registerkarte für SpamRazer-Aktualisierungen 114
Screenshot 64: Optionen für Anti-Phishing 116
Screenshot 65: Directory Harvesting-Seite 118
Screenshot 66: E-Mail-Blocklist 121
Screenshot 67: Persönliche Blocklist 123
Screenshot 68: IP-Blocklist 124
Screenshot 69: IP-DNS-Blocklist 126
Screenshot 70: URI-DNS-Blocklist 127
Screenshot 71: Sender Policy Framework aktivieren und konfigurieren 129
Screenshot 72: GFI MailEssentials Anti-Spoofing-Filter 131
Screenshot 73: E-Mail-Ausnahmen 133
Screenshot 74: Optionen der Header-Prüfung 135
Screenshot 75: Spracherkennung 137
Screenshot 76: Eigenschaften der Spam-Stichwortprüfung 138
Screenshot 77: Eigenschaften der Bayes'schen Analyse 141
Screenshot 78: Registerkarte für die Whitelist 144

Screenshot 79: Persönliche Whitelist 147
Screenshot 80: Neue Absender – Allgemein 148
Screenshot 81: Neue Absender – Ausnahmen 149
Screenshot 82: Anti-Spam-Aktionen 151
Screenshot 83: Zuweisen von Filterprioritäten 154
Screenshot 84: Eigenschaften der SMTP-Übertragungsfilterung 155
Screenshot 85: Eigenschaften des Administrator-Spam-Berichts 156
Screenshot 86: Empfänger-Spam-Bericht 157
Screenshot 87: Empfängerliste für Spam-Berichte 158
Screenshot 88: Protokollrotator 159
Screenshot 89: Globale Aktionen 160
Screenshot 90: DNS-Servereinstellungen 161
Screenshot 91: Perimeter-SMTP-Servereinstellungen 165
Screenshot 92: SpamTag-Installationssprache und -Lizenzbedingungen 170
Screenshot 93: SpamTag in Microsoft Outlook 2010 173
Screenshot 94: SpamTag in Microsoft Outlook 2003 174
Screenshot 95: Inhaltsfilterung: Registerkarte 'Textkörper' – Bedingungen festlegen 182
Screenshot 96: Inhaltsfilterung: Registerkarte 'Textkörper' – Konfigurieren weiterer Optionen 183
Screenshot 97: Inhaltsfilterung: Registerkarte „Benutzer/Ordner“ 185
Screenshot 98: Hinzufügen von Benutzern zu einer Inhaltsfilterungsregel 186
Screenshot 99: Anhangsfilterung: Registerkarte 'Allgemein' 189
Screenshot 100: Anhangsfilterung: Registerkarte für Aktionen 191
Screenshot 101: Inhaltsfilterung: Registerkarte „Benutzer/Ordner“ 193
Screenshot 102: Hinzufügen von Benutzern zu einer Inhaltsfilterungsregel 194
Screenshot 103: Hinzufügen einer neuen Regel für die erweiterte Inhaltsfilterung 196
Screenshot 104: Registerkarte für Aktionen 197
Screenshot 105: Inhaltsfilterung: Registerkarte „Benutzer/Ordner“ 199
Screenshot 106: Hinzufügen von Benutzern zu einer Inhaltsfilterungsregel 200
Screenshot 107: Prüfungen durch die Dekomprimierungs-Engine 202
Screenshot 108: Suchbereich für Malware- und Spam-E-Mails 209
Screenshot 109: Suchbereich für Malware- und Spam-E-Mails 211
Screenshot 110: Nur-Spam-Suchbereich 213
Screenshot 111: Standardmäßige und benutzerdefinierte Suchordner 214
Screenshot 112: Standardmäßige Suchordner 216
Screenshot 113: Suchergebnisse 218
Screenshot 114: Details zu Elementen in Quarantäne 219
Screenshot 115: Quarantäne-RSS-Feeds 222
Screenshot 116: Spam-Optionen – Registerkarte für allgemeine Optionen 223
Screenshot 117: Spam-Optionen – Registerkarte für Benutzereinstellungen 224
Screenshot 118: Quarantänemodus 226

Screenshot 119: Nicht vorhandene Empfänger 228
Screenshot 120: Speicherort des Quarantänespeichers und öffentliche URL 230
Screenshot 121: Hinzufügen eines neuen Haftungsausschlusses 233
Screenshot 122: HTML-Haftungsausschluss 234
Screenshot 123: Einstellungen für automatische Antwort 236
Screenshot 124: Dialogfeld für Variablen 237
Screenshot 125: Erstellen einer neuen Liste 239
Screenshot 126: Angeben der Administrator-E-Mail-Adresse 245
Screenshot 127: Scan-Manager 246
Screenshot 128: Proxy-Einstellungen für den Aktualisierungsserver 247
Screenshot 129: Liste der lokalen Domänen 248
Screenshot 130: Prüfung auf Produkt-Patches 251
Screenshot 131: Einstellungen für die Zugriffskontrolle 252
Screenshot 132: Seite mit Versionsinformationen 253
Screenshot 133: GFI MailEssentials Switchboard: UI-Modus 255
Screenshot 134: IIS-Sicherheit – Registerkarte „ACL“ 257
Screenshot 135: IIS-Sicherheit – Registerkarte „Authentifizierung“ 258
Screenshot 136: Benachrichtigungen über fehlgeschlagenen E-Mails aktivieren 260
Screenshot 137: Rückverfolgungsoptionen konfigurieren 261
Screenshot 138: Der GFI MailEssentials POP3-Downloader 263
Screenshot 139: Einwahloptionen 265
Screenshot 140: Konfigurieren eines Master-Servers 272
Screenshot 141: Konfigurieren eines Slave-Servers 274
Screenshot 142: Import-/Export-Tool für Konfigurationseinstellungen 276
Screenshot 143: Exportieren von Einstellungen über die Befehlszeile 279
Screenshot 144: Importieren von Einstellungen über die Befehlszeile 280
Screenshot 145: Das GFI MailEssentials Switchboard: Fehlerbehebung 281
Screenshot 146: Das GFI MailEssentials Switchboard: Fehlerbehebung 282
Screenshot 147: Ändern von Fernzugriffsports 284
Screenshot 148: Hinzufügen von Leistungsindikatoren für die VSAPI in Windows 2008 Server 286
Screenshot 149: Überwachung von 'Virenscanner – Gescannte Dateien' im Systemmonitor von Windows Server 2008 287

1 Einführung

1.1 Info zu diesem Handbuch

In diesem Administratorhandbuch wird erläutert, wie Sie GFI MailEssentials in Ihrem Netzwerk installieren, ausführen und konfigurieren und eventuelle Fehler beheben. In der folgenden Tabelle wird der Inhalt dieses Handbuchs beschrieben.

Kapitel	Beschreibung
Informationen	» Die Komponenten und Tools, aus denen GFI MailEssentials besteht » Funktionsweise der Scans für ein- und ausgehende E-Mails » Überblick über die Engines, die Ihre Mailsystem schützen » Typische Bereitstellungsszenarien Weitere Informationen finden Sie unter „Informationen zu GFI MailEssentials“ (Seite 12).
Installation	» Die von GFI MailEssentials unterstützten Umgebungen und E-Mail-Infrastrukturen » Produktvoraussetzungen für Ihr Netzwerk » Vorbereitung Ihrer Umgebung auf die Produktinstallation » Anleitungen zu Installation und Upgrade » Die wichtigsten Schritte zur Inbetriebnahme des Produkts mit Standardeinstellungen » Testen der Installation und Ausführen des Produkts Weitere Informationen finden Sie unter „Installation“ (Seite 21).
Statusüberwachung	» Echtzeitüberwachung des Status von GFI MailEssentials mithilfe des Dashboards » Erstellen von statistischen und grafischen Berichten zur Mailnutzung Weitere Informationen finden Sie unter „Statusüberwachung“ (Seite 53).
Benutzeraktionen	Erklärt, was Domänenbenutzer (keine Domänenadministratoren) mit GFI MailEssentials tun können » Konfigurieren persönlicher Whitelists und Blocklists » Pflegen von E-Mails in Quarantäne Weitere Informationen finden Sie unter „Endbenutzeraktionen“ (Seite 19).
E-Mail-Sicherheit	Beschreibt, wie Scan-Engines zum Schutz vor Malware konfiguriert werden. Weitere Informationen finden Sie unter „E-Mail-Sicherheit“ (Seite 73).
Anti-Spam	» Konfigurieren der Anti-Spam-Filter » Umgang mit E-Mails, die als Spam identifiziert werden » Sortieren der Scan-Reihenfolge nach Filterpriorität » Allgemeine Anti-Spam-Einstellungen » Klassifizieren von E-Mails direkt im Benutzerpostfach (Scannen öffentlicher Ordner) Weitere Informationen finden Sie unter „Anti-Spam“ (Seite 111).
Inhaltsfilterung	Beschreibt, wie Engines zum Scannen von E-Mail-Inhalten konfiguriert werden. Weitere Informationen finden Sie unter „Inhaltsfilterung“ (Seite 180).
Quarantäne	Beschreibt die Verwaltung und Verwendung der Quarantäne von GFI MailEssentials. Weitere Informationen finden Sie unter „Quarantäne“ (Seite 208).

Kapitel	Beschreibung
E-Mail-Verwaltung	Verwendung der Tools in der E-Mail-Verwaltungstools-Konsole » Haftungsausschlüsse » Automatische Antworten » Listenserver » E-Mail-Überwachung Weitere Informationen finden Sie unter „E-Mail-Verwaltung“ (Seite 232). **HINWEIS:** Über die E-Mail-Verwaltungskonsole haben Sie auch Zugriff auf die POP2Exchange-Funktion. Weitere Informationen finden Sie unter „POP2Exchange - E-Mails vom POP3-Server herunterladen“ (Seite 262).
Allgemeine Einstellungen	Beschreibt, wie Sie allgemeine Einstellungen für Ihre Umgebung anpassen. Weitere Informationen finden Sie unter „Allgemeine Einstellungen“ (Seite 245).
Diverses	Beschreibt verschiedene Funktionen und Tools, die zur Verwaltung von GFI MailEssentials verwendet werden können. Weitere Informationen finden Sie unter „Verschiedene Themen“ (Seite 253).
Fehlerbehebung	In diesem Kapitel wird beschrieben, wie Sie die häufigsten Probleme bei der Verwendung von GFI MailEssentials beheben. Weitere Informationen finden Sie unter „Fehlerbehebung und Support“ (Seite 289).

1.2 Begriffe und Konventionen dieses Handbuchs

Begriff	Beschreibung
	Zusätzliche Informationen und Referenzen, die für die ordnungsgemäße Funktion von GFI MailEssentials wichtig sind.
	Wichtige Hinweise und Warnungen bezüglich potentieller, oft auftretender Probleme
>	Schritt-für-Schritt-Anleitungen für den Zugriff auf eine Funktion.
Fetter Text	Auszuwählende Elemente wie Knoten, Menüoptionen und Befehlsschaltflächen.
Kursiver Text	Parameter und Werte, die durch einen zutreffenden Wert ersetzt werden müssen, z. B. benutzerdefinierte Pfade und Dateinamen.
`Code`	Einzugebende Textwerte, z. B. Befehle und Adressen.

Definitionen von technischen Begriffen, die in diesem Handbuch verwendet werden, finden Sie im Glossar am Ende des Handbuchs.

2 Informationen zu GFI MailEssentials

Themen in diesem Kapitel:

2.1 Komponenten von GFI MailEssentials **12**

2.2 Filterung eingehender E-Mails **14**

2.3 Filterung ausgehender E-Mails **14**

2.4 Scan- und Filter-Engines für E-Mails **15**

2.5 Typische Bereitstellungsszenarien **17**

2.6 Endbenutzeraktionen **19**

2.1 Komponenten von GFI MailEssentials

2.1.1 Scan-Engine von GFI MailEssentials

Die Scan-Engine von GFI MailEssentials analysiert den Inhalt ausgehender, eingehender und interner E-Mails mit verschiedenen Engines und Filtern. Das Ergebnis der Analyse zeigt, ob eine E-Mail blockiert oder zugelassen werden soll.

> **HINWEIS**
>
> Wird GFI MailEssentials auf Microsoft® Exchange Server 2003 installiert, wird der Informationsspeicher von Microsoft® Exchange gescannt. Bei Installation auf einem Microsoft® Exchange Server 2007/2010-Computer mit Hub-Transport- und Postfachserverrolle werden auch interne E-Mails analysiert.

2.1.2 Weboberfläche von GFI MailEssentials

Die Weboberfläche von GFI MailEssentials bietet folgende Möglichkeiten:

- E-Mail-Scan-Aktivitäten überwachen
- Scan- und Filter-Engines verwalten
- E-Mails in Quarantäne überprüfen und verarbeiten
- E-Mail-Verwaltungsfunktionen konfigurieren
- Berichte erstellen

2.1.3 GFI MailEssentials Switchboard

Verwenden Sie GFI MailEssentials Switchboard, um Folgendes zu konfigurieren:

- Wie die Benutzeroberfläche von GFI MailEssentials gestartet werden soll
- Namen der virtuellen Verzeichnisse für die Weboberfläche und für RSS festlegen
- E-Mail-Verarbeitung aktivieren/deaktivieren
- Rückverfolgung aktivieren/deaktivieren
- E-Mail-Sicherungen vor und nach der Verarbeitung einstellen
- Speicherort des Quarantänespeichers und öffentliche URL für Quarantäne festlegen

- Benutzerkonto für die Einstellung „In Exchange-Ordner verschieben“ festlegen
- Remoting-Ports festlegen
- Benachrichtigungen zu fehlgeschlagenen E-Mails aktivieren/deaktivieren

2.2 Filterung eingehender E-Mails

Mit dieser Funktion werden eingehende E-Mails gescannt und gefiltert, bevor sie an die Benutzer zugestellt werden.

Eingehende E-Mails werden an GFI MailEssentials weitergeleitet und wie folgt verarbeitet:

1. Filter auf SMTP-Ebene (Directory Harvesting, Greylist und IP- bzw. IP-DNS-Blocklist) können ausgeführt werden, bevor der E-Mail-Text empfangen wird.

2. Die E-Mail wird von Malware- und Inhaltsfilter-Engines gescannt. E-Mails, bei denen Malware erkannt wird, werden entsprechend den konfigurierten Aktionen verarbeitet. Für E-Mails, die als sicher beurteilt werden, beginnt nun die nächste Phase.

3. Es wird geprüft, ob die E-Mail an eine Liste im Listenserver adressiert ist. Wenn die E-Mail zu einer Liste gehört, wird sie vom Listenserver verarbeitet.

4. Die eingehende E-Mail durchläuft die Anti-Spam-Filter. E-Mails, die die Spam-Filter-Prüfung nicht bestehen, werden anhand der konfigurierten Anti-Spam-Aktionen verarbeitet. Für E-Mails, die alle Filter erfolgreich durchlaufen und nicht als Spam identifiziert werden, beginnt nun die nächste Phase.

5. Sofern dies konfiguriert ist, werden als Nächstes automatische Antworten an den Absender gesendet.

6. Sofern dies konfiguriert ist, wird als Nächstes die E-Mail-Überwachung mit den entsprechenden Aktionen ausgeführt.

7. Anschließend wird die E-Mail vom Filter für neue Absender geprüft.

8. Wurde die E-Mail durch keine der Scan- oder Filter-Engines blockiert, wird sie an das Postfach des Benutzers gesendet.

2.3 Filterung ausgehender E-Mails

Mit dieser Funktion werden ausgehende E-Mails von internen Benutzern verarbeitet, bevor sie über das Internet versendet werden.

Ausgehende E-Mails werden vor dem Versand an GFI MailEssentials weitergeleitet und wie folgt verarbeitet:

1. Die E-Mail wird von Malware- und Inhaltsfilter-Engines gescannt. E-Mails, bei denen Malware erkannt wird, werden entsprechend den konfigurierten Aktionen verarbeitet. Für E-Mails, die als sicher beurteilt werden, beginnt nun die nächste Phase.

2. Falls Remote-Befehle in der E-Mail vorhanden sind, werden diese geprüft und ausgeführt. Werden keine Remote-Befehle gefunden, gelangt die E-Mail in die nächste Phase.

3. Sofern dies konfiguriert ist, wird als Nächstes der entsprechende Haftungsausschluss zur E-Mail hinzugefügt.

4. Sofern dies konfiguriert ist, wird als Nächstes die E-Mail-Überwachung mit den entsprechenden Aktionen ausgeführt.

5. Falls die Auto-Whitelist aktiviert ist, wird die E-Mail-Adresse des Empfängers der Auto-Whitelist hinzugefügt. Dadurch werden automatisch die Antworten dieses Empfängers an den Absender geleitet, ohne dass auf Spam geprüft wird.

6. Die E-Mail wird an den Empfänger geschickt.

2.4 Scan- und Filter-Engines für E-Mails

GFI MailEssentials beinhaltet eine Reihe von Scan- und Filter-Engines, die verhindern, dass schädliche E-Mails, Spam und andere unerwünschte E-Mails bei den Domänenbenutzern ankommen.

2.4.1 Prüfung auf schädliche E-Mails

Die folgenden Engines scannen und blockieren E-Mails, die schädliche Inhalte aufweisen.

E-Mail-Scan-Engine	Beschreibung
Virenscan-Engines	GFI MailEssentials verwendet mehrere Anti-Virus-Engines, um eingehende, ausgehende und interne E-Mails auf Viren zu scannen. GFI MailEssentials beinhaltet die Virenscan-Engines Vipre und BitDefender. Sie können auch eine Lizenz für Norman, Kaspersky und McAfee erwerben.
Informationsspeicherschutz	Ist GFI MailEssentials auf dem Microsoft® Exchange-Server installiert, ermöglicht der Informationsspeicherschutz einen Virenscan des Microsoft® Exchange-Informationsspeichers durch die Virenscan-Engines.
Scanner für Trojaner und ausführbare Dateien	Der Scanner für Trojaner und ausführbare Dateien analysiert und ermittelt die Funktion von ausführbaren Dateien, die an E-Mails angehängt sind. Anschließend kann der Scanner alle ausführbaren Dateien, die verdächtige Aktivitäten durchführen (z. B. Trojaner), in die Quarantäne verschieben.
E-Mail-Exploit-Engine	Die E-Mail-Exploit-Engine blockiert Exploits, die in einer E-Mail eingebettet sind und auf dem Computer des Empfängers ausgeführt werden können, wenn der Benutzer entweder die E-Mail empfängt oder sie öffnet.
HTML-Bereinigung	Die HTML-Bereinigung scannt und entfernt Skript-Code im Text oder Anhang von E-Mails.

2.4.2 Inhaltsfilter-Engines

Die folgenden Engines scannen den Inhalt von E-Mails auf Parameter, die mit konfigurierten Regeln übereinstimmen.

E-Mail-Scan-Engine	Beschreibung
Stichwortfilterung	Mithilfe der Stichwortfilterung können Sie Regeln einrichten, um E-Mails auf bestimmte Stichwörter oder Wortgruppen im Text oder Betreff zu filtern.
Anhangsfilterung	Mithilfe der Anhangsfilterung können Sie Regeln erstellen, um festzulegen, welche E-Mail-Anhangstypen auf dem Mailserver zugelassen oder blockiert werden sollen.
Dekomprimierungs-Engine	Die Dekomprimierungs-Engine extrahiert und analysiert Archive (komprimierte Dateien), die an eine E-Mail angehängt sind.
Erweiterte Inhaltsfilterung	Die erweiterte Inhaltsfilterung ermöglicht das Scannen von Inhalten und Header-Daten in E-Mails anhand von konfigurierbaren Suchbedingungen und regulären Ausdrücken (Regex).

2.4.3 Anti-Spam-Filter-Engines

Die folgenden Engines scannen und blockieren Spam-E-Mails.

FILTER	BESCHREIBUNG	STANDARDMÄSSIG AKTIVIERT
SpamRazer	Eine Anti-Spam-Engine, die anhand der E-Mail-Reputation, des Nachrichtenfingerabdrucks und der Inhaltsanalyse bestimmt, ob eine E-Mail als Spam einzustufen ist.	Ja
Anti-Phishing	Blockiert E-Mails, die typische Phishing-Stichwörter oder Links enthalten, die auf bekannte Phishing-Websites verweisen.	Ja
Directory Harvesting	Directory Harvesting-Angriffe treten auf, wenn Spammer versuchen, E-Mail-Adressen zu erraten, indem sie Ihrer Domäne bekannte Benutzernamen hinzufügen. Die Mehrheit der E-Mail-Adressen existiert nicht.	Ja (nur wenn GFI MailEssentials in einer Active Directory-Umgebung installiert ist)
E-Mail-Blocklist	Die E-Mail-Blocklist ist eine von Ihnen definierte Datenbank mit E-Mail-Adressen und Domänen, von denen Sie auf keinen Fall E-Mails erhalten möchten.	Ja
IP-Blocklist	Die IP-Blocklist ist eine von Ihnen definierte Datenbank mit IP-Adressen, von denen Sie auf keinen Fall E-Mails erhalten möchten.	Nein
IP-DNS-Blocklist	Die IP-DNS-Blocklist vergleicht die IP-Adressen der sendenden Mailserver mit einer öffentlichen Liste von Mailservern, die bekanntermaßen Spam versenden.	Ja
URI-DNS-Blocklist	Stoppt E-Mails, wenn sie Links zu Domänen enthalten, die in öffentlichen Spam-URI-Blocklists aufgeführt sind.	Ja
Sender Policy Framework	Dieser Filter blockiert E-Mails von gefälschten IP-Adressen, indem er mithilfe von SPF-Einträgen prüft, ob die jeweilige Absender-IP-Adresse autorisiert ist.	Nein
Anti-Spoofing	Dieser Filter vergleicht E-Mails, deren Absenderadresse mit Ihrer eigenen Domäne übereinzustimmen scheint, mit einer Liste von IP-Adressen in GFI MailEssentials. Befindet sich die Absender-IP-Adresse nicht in der Liste mit den Server-IP-Adressen der eigenen Domäne, wird die E-Mail blockiert.	Nein
Header-Prüfung	Der Filter zur Header-Kontrolle analysiert E-Mail-Header, um Spam-Mails zu erkennen.	Ja
Spam-Stichwortprüfung	Dieser Filter ermöglicht die Erkennung von Spam auf der Basis von Stichwörtern in eingehenden E-Mails.	Nein
Bayes'sche Analyse	Ein Anti-Spam-Filter kann so trainiert werden, dass er auf der Basis von Erfahrungswerten genau bestimmen kann, ob es sich bei einer E-Mail um Spam handelt.	Nein

2.4.4 Filter auf SMTP-Ebene

Die folgenden Engines scannen und blockieren E-Mails während der SMTP-Übertragung, bevor die E-Mails den Empfänger erreichen. Weitere Informationen finden Sie unter „SMTP-Übertragungsfilterung“ (Seite 154).

FILTER	BESCHREIBUNG	STANDARDMÄSSIG AKTIVIERT
IP-Blocklist	Die IP-Blocklist ist eine von Ihnen definierte Datenbank mit IP-Adressen, von denen Sie auf keinen Fall E-Mails erhalten möchten.	Nein
Directory Harvesting	Directory Harvesting-Angriffe treten auf, wenn Spammer versuchen, E-Mail-Adressen zu erraten, indem sie Ihrer Domäne bekannte Benutzernamen hinzufügen. Die Mehrheit der E-Mail-Adressen existiert nicht.	Nein
IP-DNS-Blocklist	Die IP-DNS-Blocklist vergleicht die IP-Adressen der sendenden Mailserver mit einer öffentlichen Liste von Mailservern, die bekanntermaßen Spam versenden.	Ja
Greylist	Der Greylist-Filter blockiert temporär eingehende E-Mails von unbekannten Absendern. Zulässige Mailsysteme versuchen normalerweise, die E-Mail nach einigen Minuten erneut zu senden, Spammer hingegen ignorieren solche Fehlernachrichten einfach.	Nein

2.4.5 Weitere Engines

Die folgenden Engines tragen zur Identifizierung sicherer E-Mails bei.

FILTER	BESCHREIBUNG	STANDARDMÄSSIG AKTIVIERT
Whitelist	Die Whitelist enthält Listen von Kriterien, die zulässige E-Mails identifizieren. E-Mails, die diesen Kriterien entsprechen, werden nicht von Anti-Spam-Filtern geprüft und immer direkt dem Empfänger zugestellt.	Ja
Neue Absender	Der Filter für neue Absender identifiziert E-Mails von Absendern, an die bislang keine E-Mails gesendet wurden.	Nein

2.5 Typische Bereitstellungsszenarien

In diesem Kapitel werden die verschiedenen Szenarien für die Installation und Konfiguration von GFI MailEssentials erläutert.

2.5.1 Installation direkt auf einem Microsoft® Exchange-Server

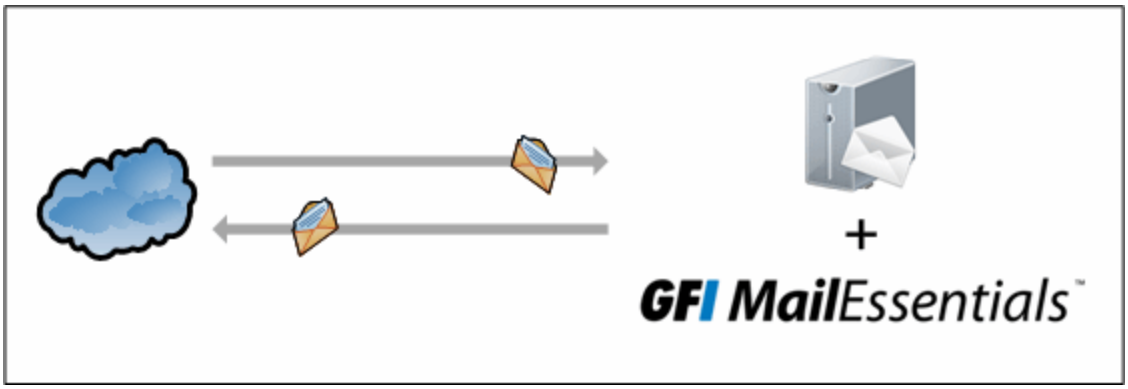


Abbildung 1: Installieren von GFI MailEssentials auf einem Microsoft® Exchange-Server

Sie können GFI MailEssentials direkt auf Microsoft® Exchange Server 2003 oder höher installieren, ohne zusätzliche Konfigurationsschritte durchzuführen.

In Microsoft® Exchange 2007/2010-Umgebungen kann GFI MailEssentials nur auf Servern mit den folgenden Rollen installiert werden:

» Edge-Serverrolle oder

» Hub-Transport-Rolle oder

» Hub-Transport- und Postfachrolle – bei dieser Konfiguration kann GFI MailEssentials auch interne E-Mails auf Viren scannen.

Unter Microsoft® Exchange 2013 kann GFI MailEssentials nur auf Servern mit der Postfachrolle installiert werden.

> **HINWEIS**
>
> GFI MailEssentials unterstützt verschiedene Mailserver, kann jedoch nur bei Microsoft® Exchange auf demselben Computer installiert werden. Bei anderen Mailservern, z. B. Lotus Domino, installieren Sie GFI MailEssentials auf einem separaten Computer.

2.5.2 Installation auf einem Mail-Gateway- oder Relay-/Perimeter-Server

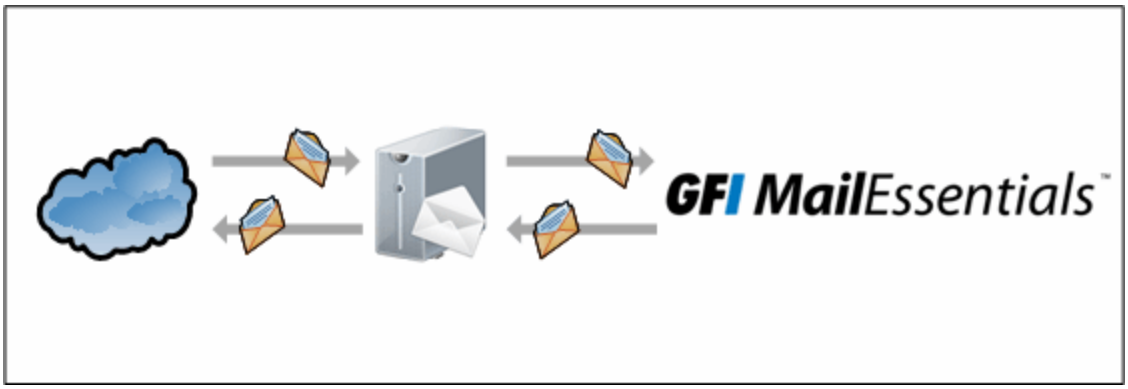


Abbildung 2: Installieren von GFI MailEssentials auf einem Mail-Gateway-/Relay-Server

Dieses Setup wird im Allgemeinen verwendet, um Spam-Nachrichten auf einem separaten Rechner zu filtern, der sich meist in einer DMZ befindet. In dieser Umgebung wird ein Server (auch Gateway-/Perimeter-Server genannt) so konfiguriert, dass er E-Mails an den Mailserver weiterleitet. GFI MailEssentials wird auf dem Gateway-/Perimeter-Server installiert, damit Spam und Malware herausgefiltert werden, bevor sie den E-Mail-Server erreichen.

Mit dieser Methode können Sie blockierte E-Mails herausfiltern, bevor diese auf dem Mailserver empfangen werden, und somit unnötigen E-Mail-Verkehr vermeiden. Sie profitieren außerdem von einer zusätzlichen Fehlertoleranz: Sollte der Mailserver ausfallen, können Sie E-Mails auch weiterhin empfangen, da diese in eine Warteschlange auf dem GFI MailEssentials-Server gestellt werden.

Bei der Installation auf einem separaten Server (also nicht auf dem Mailserver) müssen Sie diesen Computer zuerst als Gateway (auch als „Smarthost“ oder „Mail-Relay“-Server bezeichnet) konfigurieren. Das bedeutet, dass alle eingehenden E-Mails mit GFI MailEssentials gescannt werden, bevor sie zur Verteilung an den Mailserver weitergeleitet werden. Ausgehende E-Mails müssen vom Mailserver zum Scannen an den Gateway-Computer umgeleitet werden, bevor sie an den Empfänger gesendet werden.

Wenn Sie eine Firewall verwenden, sollte GFI MailEssentials idealerweise in der DMZ implementiert werden. GFI MailEssentials übernimmt bei der Installation im Perimeternetzwerk (DMZ – Demilitarized Zone) die Rolle eines Smarthost/E-Mail-Relaisservers.

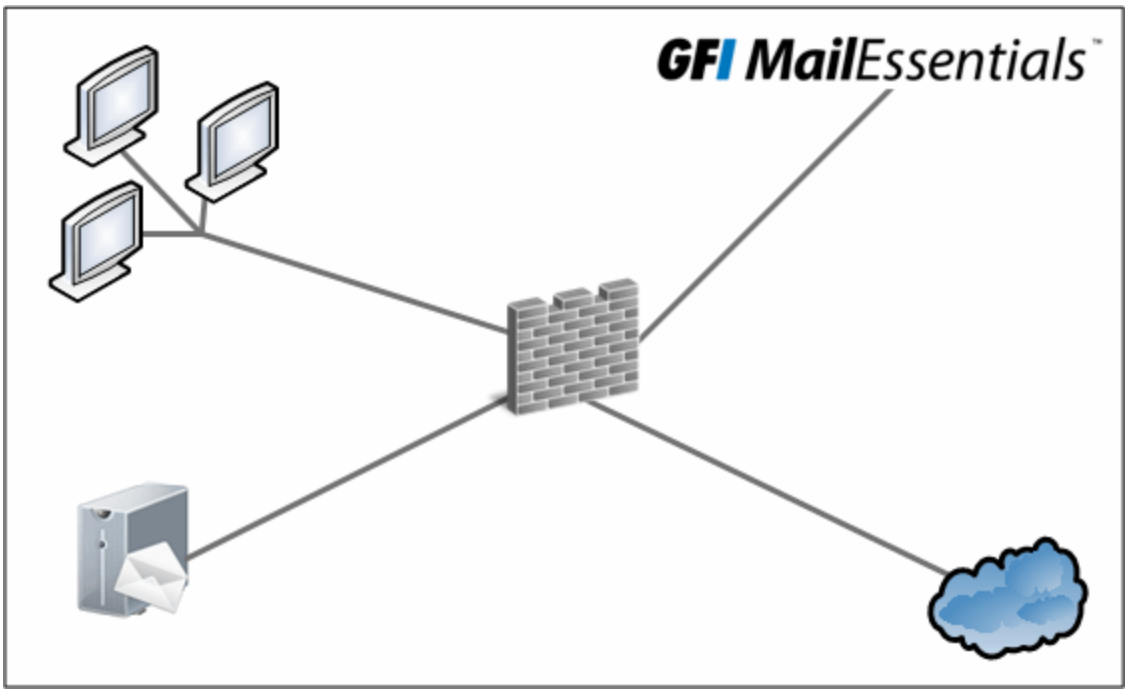


Abbildung 3: Installieren von GFI MailEssentials auf einem separaten Computer in einer DMZ

HINWEIS

Wird GFI MailEssentials auf dem Perimeter-Server installiert, können Sie die Anti-Spam-Filter verwenden, die auf SMTP-Ebene ausgeführt werden – Directory Harvesting und Greylist.

HINWEIS

In Umgebungen mit Microsoft® Exchange Server 2007/2010 kann auf Mail-Relay-Servern in einer DMZ Microsoft® Exchange Server 2007/2010 mit der Edge-Transport-Serverrolle ausgeführt werden.

HINWEIS

Konfigurieren Sie den IIS SMTP-Dienst zur Weiterleitung von E-Mails an Ihren Mailserver, und konfigurieren Sie den MX-Eintrag Ihrer Domäne so, dass er auf den Gateway-Computer verweist. Weitere Informationen finden Sie unter „Installation auf einem Mail-Gateway- oder Relay-/Perimeter-Server“ (Seite 25).

2.6 Endbenutzeraktionen

GFI MailEssentials ermittelt mithilfe von Active Directory-Gruppen, was angemeldeten Benutzern bei der Anmeldung bei GFI MailEssentials angezeigt wird. Wenn der derzeit angemeldete Benutzer zur Administrator-Gruppe gehört, wird GFI MailEssentials mit allen Konfigurationsoptionen geladen, mit denen GFI MailEssentials eingerichtet werden kann. Wenn der derzeit angemeldete Benutzer zur Benutzergruppe gehört, wird GFI MailEssentials nur mit einer eingeschränkten Anzahl an Optionen geladen, mit denen der Benutzer seinen Quarantäneordner und seine Whitelists/Blocklists verwalten kann. Der URL für die Anmeldung bei GFI MailEssentials ist immer derselbe, ob es sich beim derzeit angemeldeten Benutzer nun um ein Mitglied der Active Directory-Gruppe „Administratoren“ oder „Benutzer“ handelt.

HINWEIS

Benutzeraktionen sind nur verfügbar, wenn GFI MailEssentials für die Verwendung im IIS-Modus konfiguriert wurde. Weitere Informationen finden Sie unter „Benutzeroberflächenmodus“ (Seite 254).

Liste der verfügbaren Benutzerkontenfunktionen:

Funktion	Beschreibung
Persönliche Whitelist und Blocklist	Benutzer können eine Ergänzungsliste mit zulässigen und gesperrten E-Mail-Adressen konfigurieren, die zusätzlich zu der vom Systemadministrator eingerichteten Liste gilt. Diese Funktion steht nur bei Aktivierung der persönlichen Whitelist und/oder der persönlichen Blocklist zur Verfügung. Diese Optionen sind in der Standardeinstellung deaktiviert.
Quarantänesuche	Benutzer können Spam-E-Mails in Quarantäne verwalten. E-Mails in Quarantäne lassen sich durchsuchen, anzeigen und anschließend bestätigen oder löschen. Um diese Funktion nutzen zu können, muss die Option Aktion von Anti-Spam-Filtern so konfiguriert werden, dass Spam-E-Mails in die Quarantäne verschoben werden. Aufgrund von Sicherheitsrisiken wird Benutzern nicht gestattet, Malware-E-Mails in Quarantäne zu verwalten.
SpamTag	Über das Microsoft Outlook-Add-On SpamTag können Benutzer festlegen, wie ihre Spam-E-Mails verwaltet werden sollen. Um SpamTag über Microsoft Outlook nutzen zu können, muss es auf den Benutzercomputern installiert sein. **HINWEIS:** Diese Funktion steht Benutzern nicht über die Weboberfläche von GFI MailEssentials zur Verfügung. Weitere Informationen finden Sie unter „SpamTag für Microsoft Outlook“ (Seite 166).

Weitere Informationen über GFI MailEssentials für Endanwender finden Sie im Endbenutzerhandbuch von GFI MailEssentials.

3 Installation

Dieses Kapitel soll Ihnen helfen, GFI MailEssentials in Ihrem Netzwerk mit minimalem Konfigurationsaufwand zu installieren.

Themen in diesem Kapitel:

3.1 Systemanforderungen **21**

3.2 Aktionen vor der Installation **24**

3.3 Installationsvorgang **39**

3.4 Aktualisieren von früheren Versionen **47**

3.5 Aktionen nach der Installation **49**

3.1 Systemanforderungen

3.1.1 Hardwareanforderungen

Hardware-Mindestanforderungen für GFI MailEssentials:

3.1.2 Prozessor

» Mindestens: 1 GHz

» Empfohlen: 2 GHz mit mehreren Kernen

3.1.3 Verfügbarer Speicher (RAM)

» Mindestens: 1,2 GB

» Empfohlen: 1,5 GB

3.1.4 Freier Festplattenspeicher

» Mindestens: 6 GB

» Empfohlen: 10 GB

> **HINWEIS**
>
> Die Hardwareanforderungen hängen von verschiedenen Faktoren ab, z. B. vom E-Mail-Volumen und von der Anzahl der in GFI MailEssentials aktivierten Anti-Virus-Engines. Die oben angeführten Anforderungen gelten nur für GFI MailEssentials.

3.1.5 Softwareanforderungen

Unterstützte Betriebssysteme

» Windows® Server 2003 Standard oder Enterprise (x86 oder x64) (einschließlich R2) oder höher (einschließlich Microsoft® Windows Server 2012, Standard- und DataCenter-Versionen).

» Windows Small Business Server 2003/2008/2011

Unterstützte Mailserver

GFI MailEssentials kann auf den folgenden Mailservern ohne weitere Konfiguration installiert werden.

» Microsoft® Exchange Server 2013

HINWEIS

Informationsspeicherschutz (VSAPI) wird unter Microsoft® Exchange Server 2013 nicht unterstützt, da Microsoft VSAPI von Microsoft® Exchange Server 2013 entfernt hat.

- Microsoft® Exchange Server 2010
- Microsoft® Exchange Server 2007 SP1 oder höher
- Microsoft® Exchange Server 2003

Weitere Informationen finden Sie unter „Installation auf einem Microsoft® Exchange-Server “ (Seite 25).

GFI MailEssentials kann auch in Umgebungen mit einem beliebigen SMTP-konformen E-Mail-Server installiert werden. In diesem Fall sollte GFI MailEssentials auf dem Gateway-/Perimeter-Server installiert werden, damit Spam-Mails herausgefiltert werden, bevor sie den Mailserver erreichen.

Weitere Informationen finden Sie unter „Installation auf einem Mail-Gateway- oder Relay-/Perimeter-Server“ (Seite 25).

Unterstützte Internetbrowser

GFI MailEssentials kann mit den folgenden Internetbrowsern verwendet werden:

- Microsoft Internet Explorer 8 oder höher
- Google Chrome Version 22.0.1229.94 (10. Oktober 2012) oder höher.
- Mozilla Firefox Version 16.0.2 (26. Oktober 2012) oder höher.

Weitere erforderliche Komponenten

- Internet Information Services (IIS®) – World Wide Web-Dienst
- Internetinformationsdienste (IIS®) SMTP-Dienst – Außer bei Installation auf einem Microsoft® Exchange 2007/2010/2013-Server
- Microsoft.NET® Framework 4
- ASP.NET® 4.0
- WCF-HTTP-Aktivierung – Erforderlich bei der Verwendung des SpamTag-Plug-Ins für Microsoft Outlook
- Rollendienst für Windows®-Authentifizierung und Rollendienst für statischen Inhalt – Erforderlich bei Installation unter Microsoft® Windows Server 2008/2008 R2
- MSMQ (Microsoft® Messaging Queuing Service) – Weitere Informationen zur Installation von MSMQ finden Sie hier:

  http://go.gfi.com/?pageid=ME_MSMQ

HINWEIS

Weitere Informationen zur Installation der vorausgesetzten Komponenten unter Microsoft Windows® Server 2008 finden Sie unter:

http://go.gfi.com/?pageid=ME_Win2008

Weitere Informationen zur Installation der vorausgesetzten Komponenten unter Microsoft Windows® Server 2012 finden Sie unter:

http://go.gfi.com/?pageid=ME_Win2012

HINWEIS

Der Informationsspeicherschutz von GFI MailEssentials kann nicht verwendet werden, wenn eine andere Software zur Verwendung der Microsoft® Exchange-VSAPI registriert ist.

HINWEIS

GFI MailEssentials kann auch in virtuellen Umgebungen, z. B. mit Microsoft® Hyper-V oder VMWare-Virtualisierungssoftware, installiert werden.

» Ressource der Microsoft Virtual Server-Verbundgruppe mit Verbund aus physischen Datenträgern. Dies ist NUR für Umgebungen erforderlich, in denen Microsoft® Exchange 2003 im Cluster ausgeführt wird. Weitere Informationen finden Sie unter „Microsoft® Exchange 2003-Cluster“ (Seite 29).

HINWEIS

Weitere Informationen zum Anlegen einer Ressourcengruppe für einen Exchange Virtual Server in einem Windows Server-Verbund finden Sie unter: http://go.gfi.com/?pageid=ME_Clusterresourcegrouphowto.

3.1.6 Antiviren- und Backup-Software

Scans durch Antiviren- und Backup-Software können zu einer Fehlfunktion von GFI MailEssentials führen. Fehler treten auf, wenn diese Software den Zugriff auf bestimmte Dateien verweigert, die von GFI MailEssentials benötigt werden.

Deaktivieren Sie das Scannen der folgenden Ordner durch Antiviren- und Backup-Software von Drittanbietern:

32-Bit-Installationen (x86)	64-Bit-Installationen (x64)
<..*Programme\Gemeinsame Dateien\GFI*>	<..*Program Files (x86)\Common Files\GFI*>
<*GFI MailEssentials Installationspfad*>*GFI\MailEssentials*	
<..*Inetpub\mailroot*> - bei Installation auf einem Gateway-Rechner	
<..*Programme\Exchsrvr\Mailroot*> - bei Installation auf demselben Rechner wie Microsoft® Exchange 2003	
<..*Programme\Microsoft\Exchange Server\TransportRoles*> - bei Installation auf demselben Rechner wie Microsoft® Exchange 2007	
<..*Programme\Microsoft\Exchange Server\V14\TransportRoles*> - bei Installation auf demselben Rechner wie Microsoft® Exchange 2010	
<..*Program Files\Microsoft\Exchange Server\V15\TransportRoles*>, falls auf demselben Computer wie Microsoft® Exchange 2013 installiert	

3.1.7 Firewall-Port-Einstellungen

Konfigurieren Sie Ihre Firewall so, dass sie die Ports zulässt, die von GFI MailEssentials verwendet werden.

Port	Beschreibung
53 - DNS	Wird von folgenden Anti-Spam-Filtern verwendet: » IP-DNS-Blocklist » SpamRazer » URI-DNS-Blocklist
20 und 21 - FTP	Wird von GFI MailEssentials für die Verbindung mit **ftp.gfi.com** verwendet, um die neuesten Produktversionsinformationen abzurufen.
80 - HTTP	Wird von GFI MailEssentials zum Herunterladen von Produkt-Patch-Aktualisierungen für folgende Komponenten verwendet: » SpamRazer » Anti-Phishing » Bayes'sche Analyse » Anti-Virus-Definitionsdateien » Scanner für Trojaner und ausführbare Dateien » E-Mail-Exploit-Engine GFI MailEssentials verwendet für diese Downloads folgende Websites: » http://update.gfi.com » http://update.gfisoftware.com » http://support.gfi.com » *.mailshell.com » *.spamrazer.gfi.com **HINWEIS:** GFI MailEssentials kann auch so konfiguriert werden, dass Aktualisierungen über einen Proxy-Server heruntergeladen werden. Weitere Informationen finden Sie unter „Proxy-Einstellungen“ (Seite 246).
8013, 8015, 8021 - Remoting	Diese Ports werden für die Kommunikation zwischen Prozessen verwendet. Es ist keine Firewall-Konfiguration erforderlich, um Verbindungen mit den Remoting-Ports zu erlauben, da alle Prozesse von GFI MailEssentials auf demselben Server ausgeführt werden. **HINWEIS:** Stellen Sie sicher, dass keine anderen Anwendungen (außer GFI MailEssentials) diese Ports abhören. Falls diese Ports von anderen Anwendungen verwendet werden, können Sie die Ports ändern. Weitere Informationen finden Sie unter „Fernzugriffsports“ (Seite 283).
389/636 - LDAP/LDAPS	Dieser Port wird in folgenden Szenarien verwendet: » **Microsoft® Exchange-Umgebung** - Erforderlich, wenn der GFI MailEssentials-Server keinen Zugriff auf Active Directory hat bzw. die Benutzerliste nicht von Active Directory abrufen kann (z. B. in einer DMZ-Umgebung oder anderen Umgebung, die Active Directory nicht verwendet). » **Lotus Domino-Mailserverumgebung** - Erforderlich, um E-Mail-Adressen vom Lotus Domino-Server abzurufen. » **Andere SMTP-Mailserverumgebungen** - Erforderlich, um E-Mail-Adressen vom SMTP-Server abzurufen.

3.2 Aktionen vor der Installation

Bevor Sie GFI MailEssentials installieren, bereiten Sie Ihre Umgebung entsprechend vor.

Themen in diesem Kapitel:

» Installieren auf einem Microsoft Exchange-Server

» Installation auf einem E-Mail-Gateway- oder Relay-/Perimeter-Server

» Microsoft Exchange 2003-Cluster

» Lotus Domino

3.2.1 Installation auf einem Microsoft® Exchange-Server

Wenn Sie GFI MailEssentials auf demselben Server wie Microsoft® Exchange 2003 oder höher installieren, sind keine Aktionen oder Konfigurationen vor der Installation erforderlich.

In Microsoft® Exchange 2007/2010-Umgebungen kann GFI MailEssentials nur auf Servern mit den folgenden Rollen installiert werden:

» Edge-Serverrolle oder

» Hub-Transport-Rolle oder

» Hub-Transport- und Postfachrolle – bei dieser Konfiguration kann GFI MailEssentials auch interne E-Mails auf Viren scannen.

Unter Microsoft® Exchange 2013 kann GFI MailEssentials nur auf Servern mit der Postfachrolle installiert werden.

3.2.2 Installation auf einem Mail-Gateway- oder Relay-/Perimeter-Server

GFI MailEssentials kann auf folgende Arten installiert werden:

» Auf einem Perimeter-Server (z. B. in einer DMZ)

» Als Mail-Relay-Server zwischen dem Perimeter- (Gateway-) SMTP-Server und dem Mailserver

Dieses Setup wird im Allgemeinen verwendet, um Spam-Nachrichten auf einem separaten Rechner zu filtern, der sich meist in einer DMZ befindet. In dieser Umgebung wird ein Server (auch Gateway-/Perimeter-Server genannt) so konfiguriert, dass er E-Mails an den Mailserver weiterleitet. GFI MailEssentials wird auf dem Gateway-/Perimeter-Server installiert, damit Spam und Malware herausgefiltert werden, bevor sie den E-Mail-Server erreichen.

GFI MailEssentials verwendet den IIS SMTP-Dienst als SMTP-Server, daher muss der IIS SMTP-Dienst als Mail-Relay-Server konfiguriert werden. Gehen Sie dazu wie folgt vor:

Schritt 1: IIS SMTP-Dienst aktivieren

Schritt 2: SMTP-Domänen für die E-Mail-Weiterleitung erstellen

Schritt 3: E-Mail-Weiterleitung an Ihren Microsoft® Exchange-Server aktivieren

Schritt 4: SMTP-Mail-Relay-Server sichern

Schritt 5: Mailserver zur Weiterleitung von E-Mails über ein Gateway konfigurieren

Schritt 6: Domänen-MX-Eintrag aktualisieren, so dass er auf den Mail-Relay-Server verweist

Schritt 7: Neuen Mail-Relay-Server testen

Schritt 1: IIS SMTP-Dienst aktivieren

Windows Server 2003

1. Wählen Sie **Start > Systemsteuerung > Programme hinzufügen oder entfernen > Windows-Komponenten hinzufügen/entfernen** aus.

2. Wählen Sie **Anwendungsserver** aus, und klicken Sie auf **Details**.

3. Wählen Sie **Internetinformationsdienste (IIS)** aus, und klicken Sie auf **Details**.

4. Wählen Sie **SMTP-Dienst** aus, und klicken Sie auf **OK**.

5. Klicken Sie auf **Weiter**, um die Konfiguration abzuschließen.

Windows Server 2008

1. Starten Sie den Windows Server Manager.

2. Navigieren Sie zum Knoten **Features**, und wählen Sie **Features hinzufügen** aus.

3. Wählen Sie im **Assistenten zum Hinzufügen von Features** die Option **SMTP-Server** aus.

> **HINWEIS**
>
> Die SMTP-Server-Funktion könnte die Installation von zusätzlichen Rollendiensten und Funktionen erfordern. Klicken Sie auf **Erforderliche Rollendienste hinzufügen**, um mit der Installation fortzufahren.

4. Klicken Sie in den folgenden Bildschirmen auf **Weiter**, um erforderliche Rollendienste und Funktionen zu konfigurieren. Klicken Sie auf **Installieren**, um die Installation zu starten.

5. Klicken Sie auf **Schließen**, um die Konfiguration abzuschließen.

Schritt 2: SMTP-Domänen für die E-Mail-Weiterleitung erstellen

1. Navigieren Sie zu **Start > Systemsteuerung > Verwaltung > Internetinformationsdienste (IIS)-Manager**.

2. Erweitern Sie im linken Bereich den entsprechenden Serverknoten. Klicken Sie mit der rechten Maustaste auf **Virtueller Standardserver für SMTP**, und wählen Sie **Eigenschaften** aus.

4. Erweitern Sie den Knoten **Virtueller Standardserver für SMTP**.

5. Klicken Sie mit der rechten Maustaste auf **Domänen**, und wählen Sie **Neu > Domäne** aus.

6. Wählen Sie **Remote** aus, und klicken Sie auf **Weiter**.

7. Geben Sie den Domänennamen des Unternehmens an (z. B. test.mydomain.com), und klicken Sie auf **Fertig stellen**.

Schritt 3: E-Mail-Weiterleitung an Ihren Microsoft® Exchange-Server aktivieren

1. Klicken Sie mit der rechten Maustaste auf die neue Domäne, und wählen Sie **Eigenschaften** aus.

2. Wählen Sie **Relay eingehender Nachrichten an diese Domäne erlauben** aus.

3. Wählen Sie **Gesamte E-Mail an Smarthost weiterleiten** aus, und geben Sie die IP-Adresse des Servers an, der die E-Mails in dieser Domäne verwaltet. Die IP-Adresse muss in eckigen Klammern angegeben werden, z. B. `[123.123.123.123]`, um sie von allen DNS-Suchen auszuschließen.

4. Klicken Sie auf **OK**, um die Konfiguration abzuschließen.

Schritt 4: SMTP-Mail-Relay-Server sichern

Ein ungesicherter Mail-Relay-Server kann als offenes Relay für Spam ausgenutzt werden. Um dies zu verhindern, sollten Sie angeben, welche Mailserver E-Mails über diesen Mail-Relay-Server weiterleiten dürfen (erlauben Sie beispielsweise nur bestimmten Servern, diese E-Mail-Weiterleitung zu nutzen). Gehen Sie dazu wie folgt vor:

1. Navigieren Sie zu **Start > Systemsteuerung > Verwaltung > Internetinformationsdienste (IIS)-Manager**.

2. Erweitern Sie im linken Bereich den entsprechenden Serverknoten. Klicken Sie mit der rechten Maustaste auf **Virtueller Standardserver für SMTP**, und wählen Sie **Eigenschaften** aus.

3. Wählen Sie auf der Registerkarte **Zugriff** die Option **Relay** aus.

4. Wählen Sie die Option **Nur Computer in der Liste**, und klicken Sie auf **Hinzufügen**.

5. Geben Sie die IP-Adressen der internen Mailserver an, die E-Mails über Ihren Mail-Relay-Server weiterleiten dürfen. Sie können Folgendes angeben:

» Einzelne Computer – Autorisieren Sie einen bestimmten Computer, E-Mails über diesen Server weiterzuleiten. Verwenden Sie die DNS-Lookup-Schaltfläche, um nach der IP-Adresse eines bestimmten Hosts zu suchen.

» Gruppe von Computern – Autorisieren Sie bestimmte Computer, E-Mails über diesen Server weiterzuleiten.

» Domäne – Erlauben Sie allen Computern in einer bestimmten Domäne, E-Mails über diesen Server weiterzuleiten.

> **HINWEIS**
>
> Die Option **Domäne** verursacht eine zusätzliche Verarbeitungslast, die die Leistung des SMTP-Dienstes beeinträchtigen kann. Der Grund dafür ist, dass für alle IP-Adressen (innerhalb dieser Domäne), die E-Mails über diesen Relay-Server weiterleiten möchten, ein Reverse DNS Lookup ausgelöst wird.

Schritt 5: Mailserver zur Weiterleitung von E-Mails über GFI MailEssentials konfigurieren

Microsoft® Exchange Server 2003

Richten Sie SMTP-Connectors ein, die alle E-Mails an GFI MailEssentials weiterleiten.

1. Starten Sie den **Exchange-System-Manager**.

2. Klicken Sie mit der rechten Maustaste auf **Connectors**, klicken Sie auf **Neu > SMTP-Connector**, und geben Sie einen Connector-Namen an.

3. Wählen Sie **Gesamte Mail über diesen Connector an diese Smarthosts weiterleiten** aus, und geben Sie die IP-Adresse Ihres GFI MailEssentials-Relay-Servers in eckigen Klammern an, z. B. `[123.123.1.123]`.

4. Klicken Sie auf **Hinzufügen**, und wählen Sie den Mail-Relay-Server von GFI MailEssentials aus.

5. Klicken Sie auf **OK**.

6. Wählen Sie die Registerkarte **Adressraum** aus.

7. Klicken Sie auf **Hinzufügen**, wählen Sie **SMTP** aus, und klicken Sie auf **OK**.

8. Geben Sie den Domänennamen ein, und klicken Sie auf **OK**.

9. Wählen Sie **Weiterleitung von Nachrichten an diese Domänen erlauben** aus.

10. Klicken Sie auf **OK**.

Lotus Notes

Weitere Informationen zum Einrichten des Lotus Domino-Routing finden Sie unter Installationshandbuch (Domino).

SMTP/POP3-Mailserver

Konfigurieren Sie Ihren Mailserver so, dass alle eingehenden und ausgehenden E-Mails über GFI MailEssentials weitergeleitet werden. Verwenden Sie im Konfigurationsprogramm Ihres Mailservers die Option zur Weiterleitung aller ausgehenden E-Mails über einen anderen Mailserver. Diese Option heißt beispielsweise **Forward all messages to host (Alle Nachrichten an Host weiterleiten)** oder ähnlich. Geben Sie den Namen oder die IP-Adresse des Rechners ein, auf dem GFI MailEssentials ausgeführt wird. Speichern Sie die neuen Einstellungen, und starten Sie Ihren Mailserver neu.

Schritt 6: Domänen-MX-Eintrag aktualisieren, so dass er auf den Mail-Relay-Server verweist

Aktualisieren Sie den MX-Eintrag Ihrer Domäne so, dass er auf die IP-Adresse des neuen Mail-Relay-Servers verweist. Wird Ihr DNS-Server von Ihrem Internet Service Provider (ISP) verwaltet, muss dieser den MX-Eintrag für Sie aktualisieren.

> **HINWEIS**
>
> Wird der MX-Eintrag nicht aktualisiert, werden alle E-Mails direkt an Ihren Mailserver geleitet und gelangen somit nicht zu GFI MailEssentials.

Erfolgreiche Aktualisierung des MX-Eintrags überprüfen

So überprüfen Sie, ob der MX-Eintrag aktualisiert wurde:

1. Geben Sie in der Befehlszeile `nslookup` ein, und drücken Sie die **Eingabetaste**.
2. Geben Sie `set type=mx` ein, und drücken Sie die **Eingabetaste**.
3. Geben Sie Ihren E-Mail-Domänennamen an, und drücken Sie die **Eingabetaste**.

Der MX-Eintrag sollte die IP-Adressen der Mail-Relay-Server anzeigen.

Schritt 7: Neuen Mail-Relay-Server testen

Bevor Sie mit der Installation von GFI MailEssentials beginnen, stellen Sie sicher, dass Ihr neuer Mail-Relay-Server korrekt arbeitet.

Eingehende IIS SMTP-Verbindung testen

1. Senden Sie von einem externen Konto (z. B. einem Gmail-Konto) eine E-Mail an eine interne E-Mail-Adresse.
2. Vergewissern Sie sich, ob der beabsichtigte Empfänger die Testnachricht in seinem E-Mail-Client erhalten hat.

Ausgehende IIS SMTP-Verbindung testen

1. Senden Sie von einem internen E-Mail-Konto eine E-Mail an ein externes Konto (z. B. ein Gmail-Konto).
2. Vergewissern Sie sich, ob der beabsichtigte Empfänger die Test-E-Mail erhalten hat.

HINWEIS

Sie können auch Telnet verwenden, um die Test-E-Mail manuell zu senden und zusätzliche Fehlerbehebungsinformationen zu erhalten. Weitere Informationen finden Sie unter:

http://go.gfi.com/?pageid=ME_TelnetPort25

3.2.3 Microsoft® Exchange 2003-Cluster

Dieses Thema enthält Anleitungen zur Installation und Deinstallation von GFI MailEssentials in einem Microsoft® Exchange 2003-Clustern.

Ein Verbund ist eine Gruppe von Servern, hier als Knoten bezeichnet, die zusammen wie ein einzelner Server arbeiten. Eine solche Umgebung bietet Mechanismen für die Hochverfügbarkeit und Ausfallsicherheit, um die dauerhafte Verfügbarkeit von Ressourcen und Anwendungen, einschließlich E-Mail-Infrastrukturen sicherzustellen. Fällt ein Knoten im Verbund aus/ist nicht verfügbar, wechseln die Ressourcen und Anwendungen zu einem anderen Verbundknoten.

HINWEIS

GFI MailEssentials kann nur in einer Aktiv-Passiv-Verbundumgebung installiert werden. In einem Aktiv/Passiv-Verbund stellt ein Ausfallsicherheitsmechanismus sicher, dass beim Ausfall eines aktiven Knotens einer der verfügbaren passiven Knoten aktiv wird (also die Rolle des ausgefallenen Knotens übernimmt).

Um GFI MailEssentials in einem Microsoft® Exchange Server 2000/2003-Verbund zu installieren, sollte Folgendes gewährleistet sein:

» Alle aktiven Anwendungen werden geschlossen.

» Microsoft® Exchange Server 2000/2003 wird im Verbundmodus installiert.

» Es ist eine Ressource als Exchange Virtual Server-Verbundgruppe vorhanden, zu der unter anderem eine Verbundressource mit physischem Datenträger gehört.

» Alle Verbundknoten außer dem Knoten, auf dem GFI MailEssentials als erstes installiert wird, sollten ausgeschaltet werden.

1. Starten Sie die Installation und vergewissern Sie sich, dass:

» Alle Dateien auf der gemeinsamen Festplatte installiert werden

» Sie installieren auf der Standard-Website des Computers

2. Starten Sie mit dem IIS Manager nach Abschluss der Installation die Standard-Website.

3. Wählen Sie **Systemsteuerung > Verwaltung > Verbundadministrator** und legen Sie eine neue Ressourcengruppe an (klicken Sie mit der rechten Maustaste auf **Gruppen > Neu > Gruppe**).

4. Geben Sie als Namen `GFI MailEssentials` und als Beschreibung `Dienste für GFI MailEssentials` ein. Klicken Sie auf **Weiter**.

5. Verschieben Sie alle verfügbaren Knoten in **Bevorzugte Besitzer** und klicken Sie auf **Fertig stellen**.

6. Klicken Sie mit der rechten Maustaste auf **GFI MailEssentials > Neu > Ressource**.

7. Stellen Sie als Namen `GFI-Listenserver` ein.

8. Stellen Sie als Ressourcentyp: Generischer Dienst ein und klicken Sie auf **Weiter**.

9. Richten Sie alle verfügbaren Knoten für mögliche Besitzer ein und klicken Sie auf **Weiter**.

10. Klicken Sie auf **Weiter**.

11. Legen Sie als Dienstnamen `listserv` fest und klicken Sie auf Weiter.

12. Klicken Sie auf **Fertig stellen**.

13. Wiederholen Sie die Schritte 7 bis 12 mit den folgenden Daten:

Name	Dienstname
GFI MailEssentials AntiSpam Attendant	gfiasmlhost
GFI MailEssentials AS-Scan-Engine	gfiscans
GFI MailEssentials Auto-Updater	msecavupdate
GFI MailEssentials AV-Scan-Engine	gfiscanm
GFI MailEssentials EmailSecurity Attendant	msecmlhost
GFI MailEssentials Enterprise-Übertragung	gfimetrxsvc
GFI MailEssentials Legacy Attendant	gfiasmsecatt
GFI MailEssentials LocalMode Host	csecmlhost
GFI POP2Exchange	gfipop2exch

14. Stellen Sie zum Abschluss die GFI MailEssentials-Gruppe online.

15. Schalten Sie diesen Knoten aus und starten Sie einen neuen Knoten.

16. Wiederholen Sie die Schritte 1 und 2 für alle Verbundknoten.

Deinstallieren von GFI MailEssentials in einer Cluster-Umgebung

Stellen Sie sicher, dass nur ein einzelner Cluster-Knoten eingeschaltet wird und dass alle anderen ausgeschaltet sind.

1. Beenden Sie alle GFI-Dienste.

2. Sichern Sie den gesamten Inhalt GFI MailEssentials-Installationsordners an einem anderen Speicherort.

3. Löschen Sie alle GFI-Dienste der Verbundressourcen aus der Gruppe GFI MailEssentials.

4. Starten Sie alle GFI-Dienste und stellen Sie sicher, dass alle Verbunddienste und Exchange-Dienste aktiv sind.

5. Beginnen Sie bei der Deinstallation mit dem ersten Knoten.

6. In der Eingabeaufforderung

» Geben Sie `sc delete msecavupdate` ein und drücken Sie die **Eingabetaste**.

» Geben Sie `sc delete gfiasmsecatt` ein und drücken Sie die **Eingabetaste**.

7. Klicken Sie auf **Start > Run (Ausführen)**, und geben Sie `regedit` ein. Drücken Sie die **Eingabetaste**.

8. Löschen Sie den Schlüssel `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\GFI`

9. Kopieren Sie die Sicherungskopie von GFI MailEssentials zum Installationsort.

10. Schalten Sie den aktuellen Knoten aus und starten Sie den nächsten Knoten. Stellen Sie sicher, dass alle Verbunddienste, Exchange-Dienste und GFI MailEssentials-Dienste aktiv sind.

11. Deinstallieren Sie GFI MailEssentials.

12. In der Eingabeaufforderung:

» Geben Sie `sc delete msecavupdate` ein und drücken Sie die **Eingabetaste**.

» Geben Sie `sc delete gfiasmsecatt` ein und drücken Sie die **Eingabetaste**.

13. Wiederholen Sie die Schritte 7 bis 12 für die restlichen Knoten.

14. Löschen Sie den GFI MailEssentials -Installationsordner und die Sicherungskopie. Löschen Sie im Verbundadministrator alle GFI-Dienste.

3.2.4 Lotus Domino

Informationen zur Verwendung von GFI MailEssentials mit Lotus Domino.

» Lotus Domino-Inkompatibilitäten

» Installationsinformationen für Lotus Domino

» Konfiguration des Lotus Domino Anti-Spam-Ordners

Lotus Domino-Inkompatibilitäten

Interne Memos/E-Mails werden nicht gescannt

GFI MailEssentials scannt keine internen Memos/E-Mails von Lotus Domino, da das Absender-/Empfängerformat nicht kompatibel ist. Wenn GFI MailEssentials interne Memos/E-Mails empfängt, werden sie in die Warteschlange gestellt und nicht verarbeitet.

> **HINWEIS**
> Leiten Sie keine internen Memos/E-Mails an GFI MailEssentials weiter.

GFI MailEssentials-Listenserver funktioniert nicht mit Lotus Domino

Das Erstellen von Newslettern oder Diskussionslisten funktioniert nicht in der internen Domäne von Lotus Domino. Diese Option sollte nicht verwendet werden. Andernfalls können Lotus Domino-Benutzer keine E-Mails an die Liste senden.

GFI MailEssentials Installationshandbuch für Lotus Domino

Die Angaben in diesem Abschnitt helfen Ihnen dabei, Lotus Domino mit GFI MailEssentials zu installieren und zu konfigurieren. Installieren Sie GFI MailEssentials auf einem separaten Rechner ohne Lotus Domino (siehe unten stehende Abbildung).

Abbildung 4: Installation von GFI MailEssentials auf einemseparaten Server ohne Lotus Domino

Installieren Sie GFI MailEssentials, indem Sie die Installationsdatei von GFI MailEssentials ausführen und den Anleitungen am Bildschirm folgen. Weitere Informationen finden Sie unter „Installation“ (Seite 21).

Wenn GFI MailEssentials auf einem Rechner mit Active Directory installiert ist, wird möglicherweise das unten stehende Dialogfeld angezeigt. Wählen Sie Select **Nein, ich habe kein Active Directory…**, um GFI MailEssentials im SMTP-Modus zu installieren.

Konfigurieren Sie den Computer, auf dem GFI MailEssentials installiert ist, als Gateway (auch als „Smarthost“ oder „Mail-Relay“-Server bezeichnet) für alle E-Mails. Das bedeutet, dass alle eingehenden E-Mails diesen Computer passieren müssen, bevor sie zur Verteilung an den Mailserver weitergeleitet werden (alle E-Mails and Ihren Mailserver kommen zunächst auf diesem Computer an).

Das Gleiche gilt für ausgehende E-Mails. Auch sie müssen vom Mailserver zum Scannen an den Gateway-Computer umgeleitet werden, bevor sie über das Internet an externe Empfänger gesendet werden (der letzte „Halt“ von E-Mails, die über das Internet gesendet werden, ist dieser Computer). Auf diese Weise überprüft GFI MailEssentials alle ein- und ausgehenden E-Mails bei der Zustellung an den Empfänger.

Der MX-Eintrag der Domäne muss auf den Mail-Relay-Server verweisen

> **HINWEIS**
>
> Wenn Sie den DNS-Server nicht selbst verwalten, bitten Sie Ihren ISP, diese Änderung durchzuführen.

Da der neue Mail-Relay-Server als erster alle eingehenden E-Mails empfangen muss, ist der MX-Eintrag Ihrer Domäne zu aktualisieren, damit er auf die IP-Adresse des neuen Mail-Relay-/Gateway-Servers verweist.

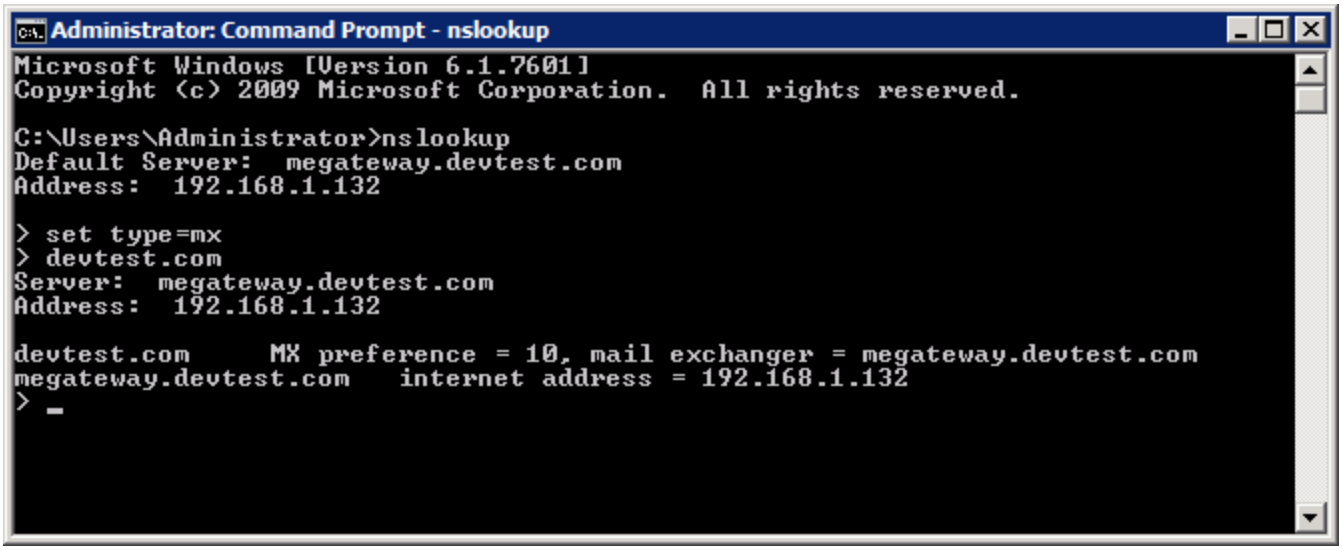
Prüfen Sie den MX-Eintrag Ihrer Domäne wie folgt:

1. Geben Sie in der Befehlszeile `nslookup` ein und drücken Sie die **Eingabetaste**.

2. Geben Sie `set type=mx` ein und drücken Sie die **Eingabetaste**.

3. Geben Sie Ihre E-Mail-Domäne ein und drücken Sie die **Eingabetaste**.

Der MX-Eintrag sollte eine einzige IP-Adresse zurückgeben, nämlich die IP-Adresse des Computers, auf dem GFI MailEssentials ausgeführt wird.



Screenshot 1: Prüfen des MX-Eintrags des DNS

4. Testen Sie den neuen Mail-Relay-Server. Bevor Sie mit der Installation von GFI MailEssentials beginnen, stellen Sie sicher, dass der neue Mail-Relay-Server ordnungsgemäß funktioniert.

5. Testen Sie die eingehende IIS-SMTP-Verbindung des E-Mail-Relaisservers, indem Sie eine E-Mail von einem externen Konto an einen internen Benutzer senden (falls Sie kein externes Konto haben, können Sie auch ein Webmail-Konto wie z. B **mail.live.com** verwenden). Stellen Sie sicher, dass die Nachricht vom E-Mail-Client empfangen wurde.

6. Testen Sie die ausgehende IIS-SMTP-Verbindung des Mail-Relay-Servers, indem Sie eine E-Mail von einem E-Mail-Client an ein externes Konto senden. Stellen Sie sicher, dass der externe Empfänger die E-Mail erhalten hat.

> **HINWEIS**
>
> Statt eines E-Mail-Clients können Sie die E-Mail auch manuell über Telnet senden. Diese Möglichkeit bietet Ihnen auch mehr Informationen zur Lösung eventuell auftretender Probleme.

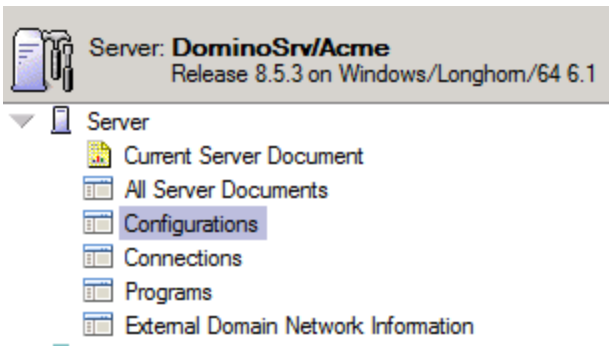
Weitere Informationen hierzu finden Sie unter:

http://support.microsoft.com/support/kb/articles/Q153/1/19.asp

Konfigurieren von Lotus Domino zum Versenden ausgehender E-Mails über GFI MailEssentials

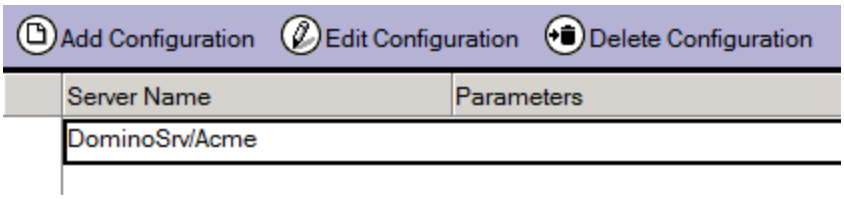
Um alle ausgehenden E-Mails an den Server zu leiten, auf dem GFI MailEssentials installiert ist, muss Lotus Domino wie folgt konfiguriert werden.

1. Klicken Sie in Lotus FormDomino Administrator auf die Registerkarte **Configuration (Konfiguration)** und wählen Sie **Server > Configurations (Konfigurationen)**.



Screenshot 2: Lotus Domino Administrator: Klicken auf die Option „Configurations“ („Konfigurationen“)

2. Nach Auswahl des Konfigurationsbereichs zeigt das Hauptfenster die Konfiguration des Servers an. Wählen Sie den gewünschten Server aus und klicken Sie auf **Edit Configuration (Konfiguration bearbeiten)**.

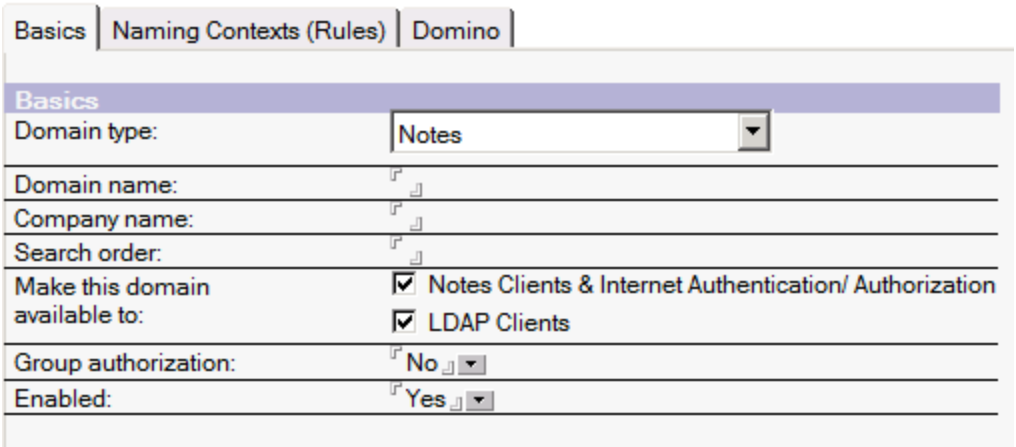


Screenshot 3: Klicken auf die Option „Edit Configuration“ („Konfiguration bearbeiten“)

Wählen Sie auf der Seite des Konfigurationsdokuments die Registerkarte **Router/SMTP** und stellen Sie sicher, dass die Option **Basics** ausgewählt ist. Doppelklicken Sie auf die Inhalte, um den Bearbeitungsmodus zu aktivieren. Wählen Sie die Option **Relay host for messages leaving the local internet domain (Umleitungshost für Nachrichten, die die lokale Internetdomäne verlassen)** und geben Sie die IP-Adresse des Computers ein, auf dem GFI MailEssentials installiert ist. Klicken Sie auf **Save and Close (Speichern und schließen)**, um das Konfigurationsdokument zu speichern.

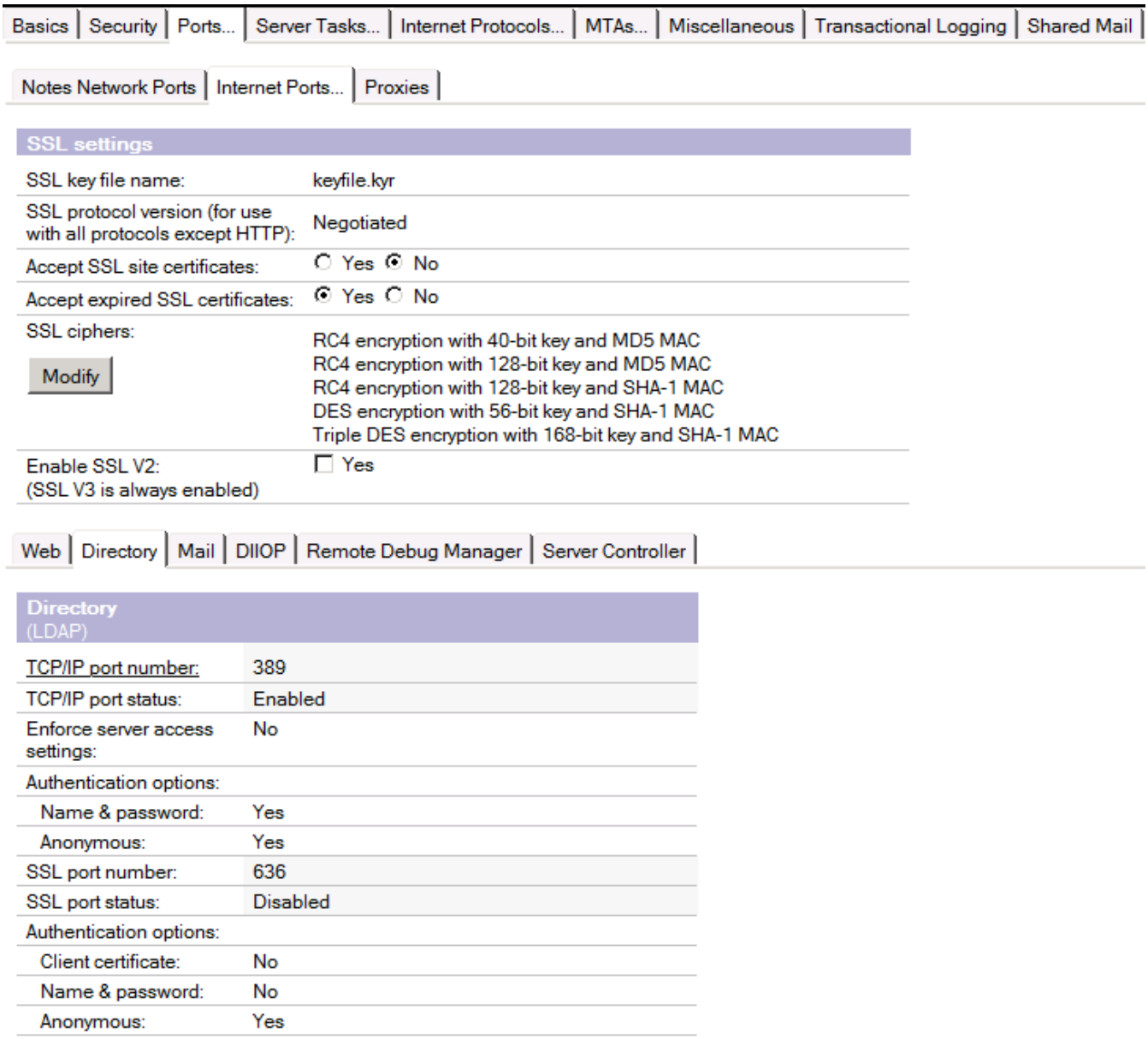
LDAP-Einstellungen von Lotus Domino

Aktivieren Sie in Lotus Domino die Optionen „Directory Catalog“ und „Directory Assistance“. Klicken Sie in der Datenbank von Directory Assistance auf **Add Directory Assistance (Dirfectory Assistance hinzufügen)**, um ein neuens Assistance-Dokument anzulegen. Im Dokument müssen Sie die LDAP-Clients unter **Make this domain available to (Diese Domäne verfügbar machen für)** wie folgt:-



Screenshot 4: LDAP-Einstellungen von Lotus Domino

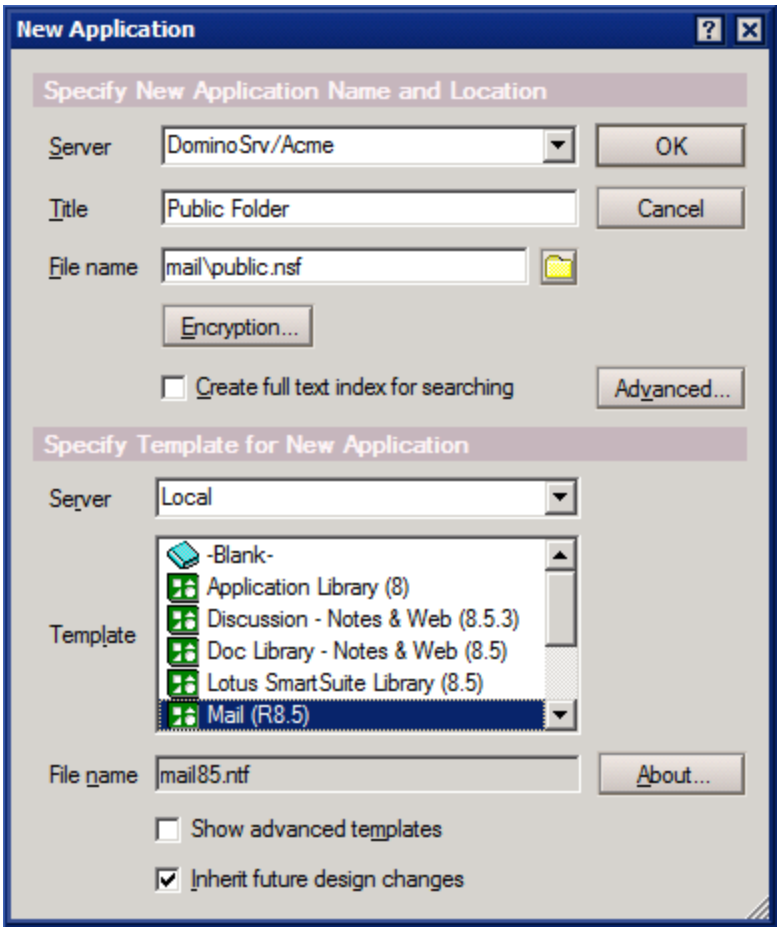
In der Serverkonfiguration müssen die Anmeldedaten bearbeitet werden. Die anonyme Authentifizierung muss aktiviert werden, damit GFI MailEssentials auf Lotus Domino LDAP zugreifen kann.



Screenshot 5: Anonyme Authentifizierung aktivieren

Konfiguration des Lotus Domino Anti-Spam-Ordners

1. Legen Sie im Lotus Notes Administrator eine Datenbank mit der normalen MAIL85.NTF-Vorlage an, die als öffentlicher Ordner verwendet wird. Klicken Sie nach dem Anlegen der Datenbank mit der rechten Maustaste im Dateibereich darauf, und wählen Sie **Access Control (Zugriffssteuerung)**. Konfigurieren Sie den Benutzer, die Gruppe oder den Server für den Zugriff auf die Datenbank.



Screenshot 6: Eine neue Datenbank anlegen

2. Geben Sie in der Serverkonsole Folgendes ein, um die Datenbank zu konvertieren:

```
load convert -e -h mail\public.nsf
```

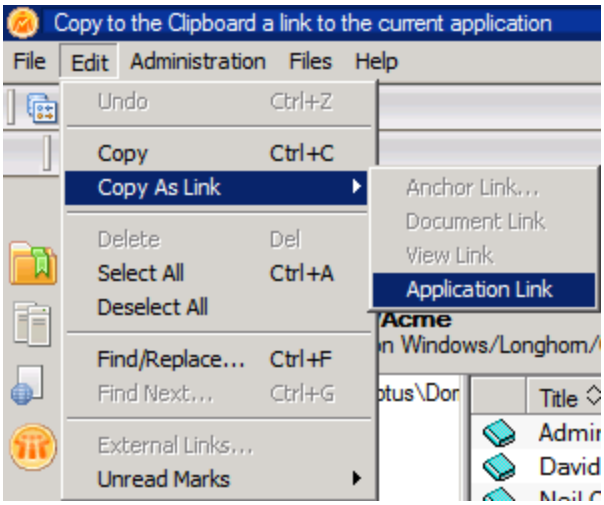
Nach Eingabe des Befehls sollten die folgenden Ergebnisse angezeigt werden:

```
load convert -e -h mail\public.nsf

[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Conversion Utility starting
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Started enabling NSF support for IMAP
in 'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Finished enabling NSF support for IMAP
in 'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Started adding IMAP specific items in
'mail\public.nsf'
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Convert: Finished adding IMAP specific items in
'mail\public.nsf'. 0 messages succeeded, 0 messages failed.
[0A34:0002-06F4] 19/09/2012 16:48:43   Mail Conversion Utility shutdown
```

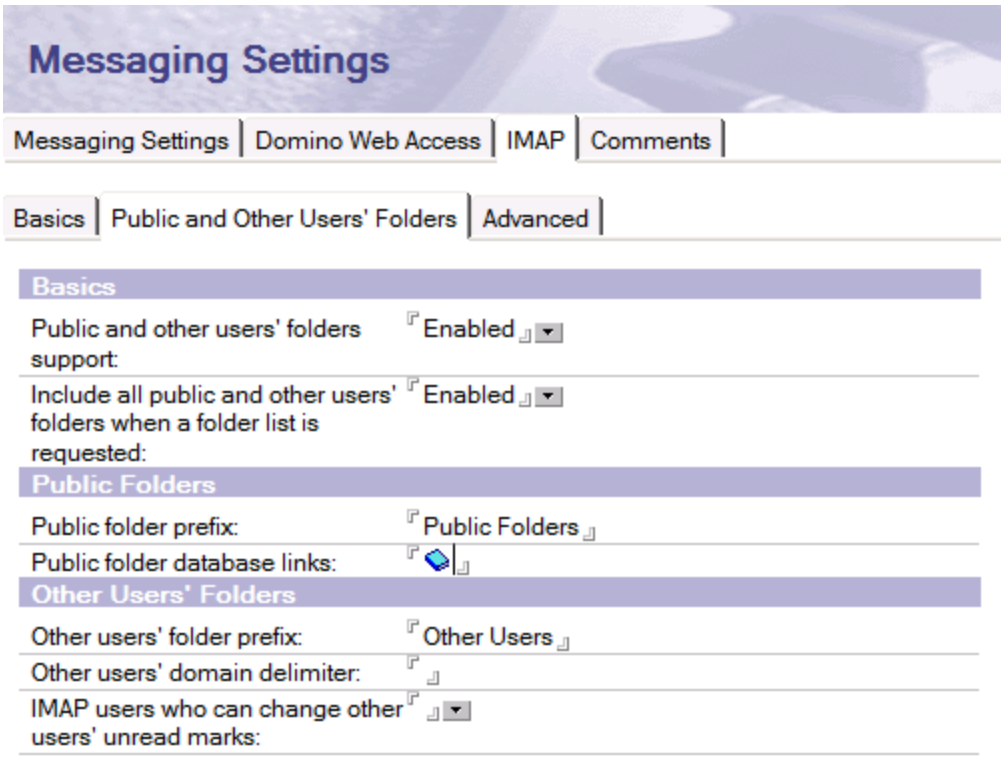
Screenshot 7: Konvertierungsergebnis laden

3. Stellen Sie nach Abschluss des Vorgangs sicher, dass über den IMAP-Dienst auf die Datenbank zugegriffen werden kann. Wählen Sie im Lotus Notes Administrator die Option **Configuration (Konfiguration)** und anschließend die Registerkarte **Files (Dateien)** aus. Markieren Sie die Datenbank des öffentlichen Ordners, klicken Sie auf **Edit (Bearbeiten)**, wählen Sie **Copy as Link (Als Link kopieren)**, und klicken Sie auf **Application Link (Anwendungslink)**.



Screenshot 8: Einen Link zur aktuellen Anwendung in die Zwischenablage kopieren

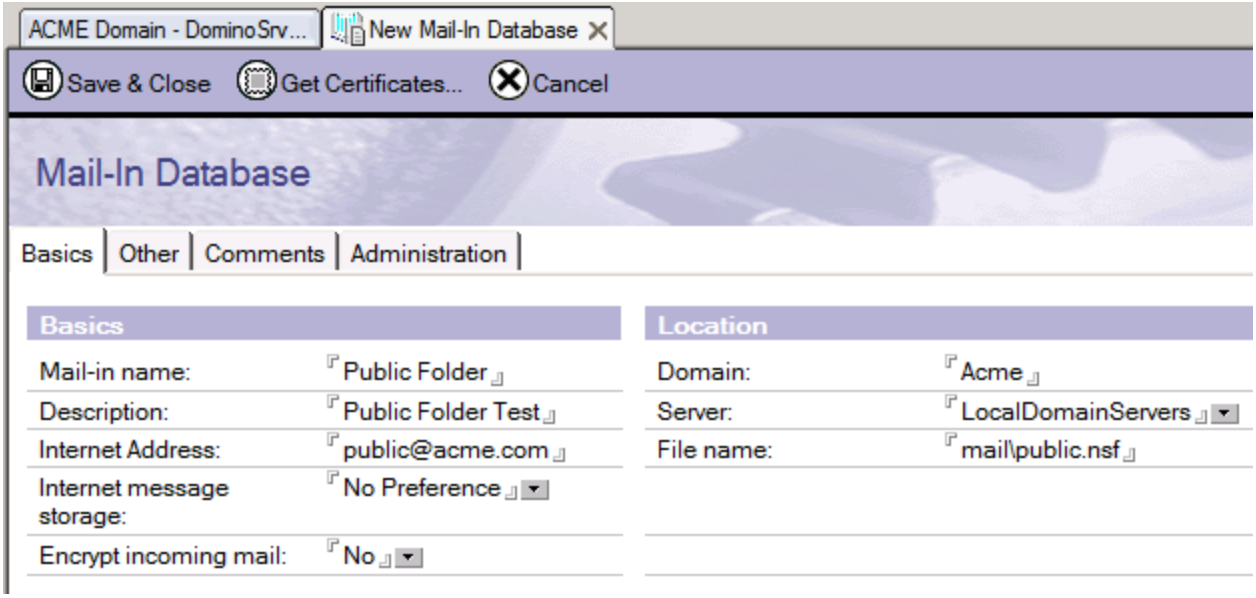
4. Wählen Sie in der Konfiguration **Messaging Settings (Nachrichteneinstellungen)** die Registerkarte **IMAP** aus.



Screenshot 9: Bei Anforderung einer Ordnerliste alle öffentlichen Ordner und Ordner anderer Benutzer einbeziehen

5. Wählen Sie die Registerkarte **Public and Other Users' Folders (Öffentliche Ordner und Ordner anderer Benutzer)** aus. Klicken Sie mit der rechten Maustaste und fügen Sie den Link in die **Public Folders Database Links (Datenbanklinks öffentlicher Ordner)** ein, und aktivieren Sie die Option **Include all public and other users folders when a folder list is requested (Bei Anforderung einer Ordnerliste alle öffentlichen Ordner und Ordner anderer Benutzer einbeziehen)**.

6. Speichern und schließen Sie das Dokument.



Screenshot 10: Neue Eingangs-E-Mail-Datenbank

7. Konfigurieren Sie im Lotus Notes Administrator den Ordner für die E-Mail-Nutzung. Wählen Sie **People and Groups (Personen und Gruppen)** und dann **Mail-In Database (Eingangs-E-Mail-Datenbank)**. Erstellen Sie eine neue Eingangs-E-Mail-Datenbank, und geben Sie den vollständigen Verzeichnispfad an (z. B. Mail\public.nsf).

8. Speichern und schließen Sie das Dokument.

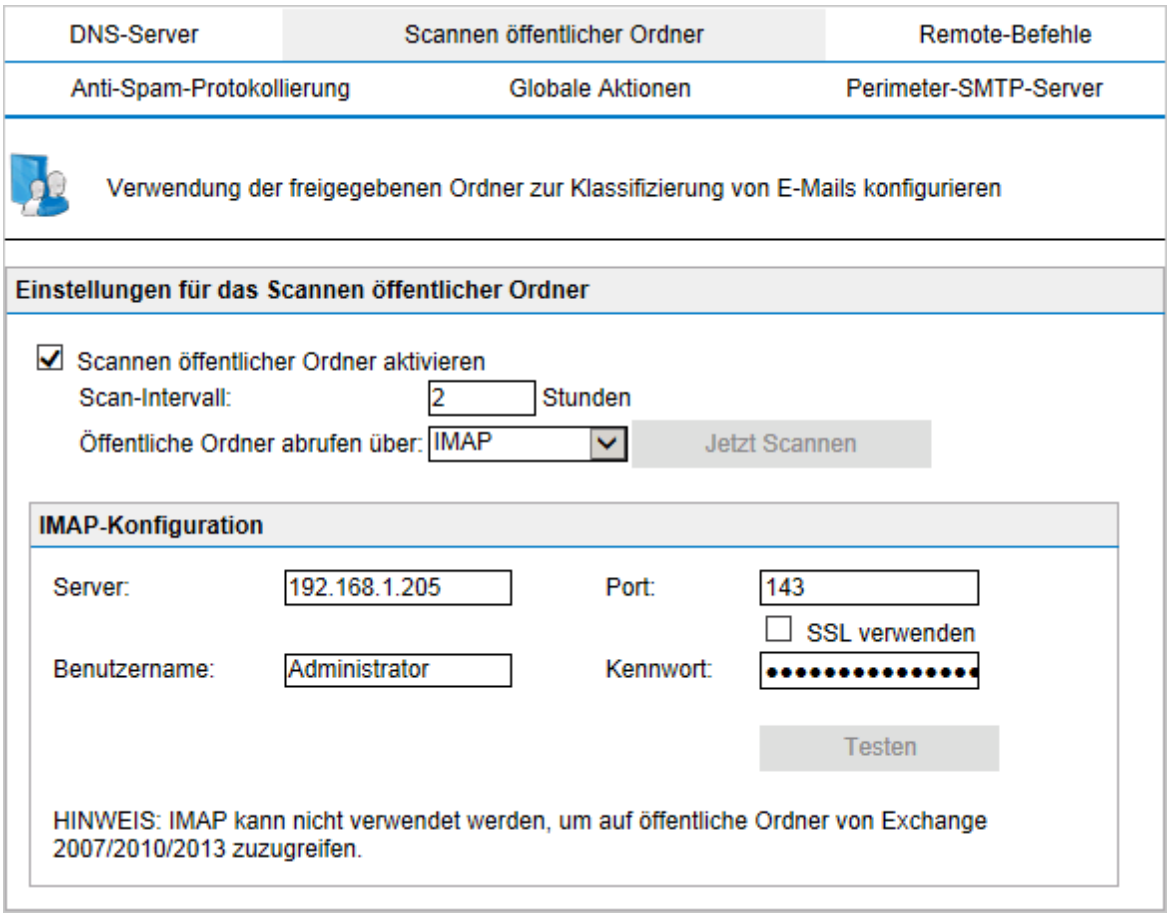
9. Erweitern Sie auf der GFI MailEssentials-Weboberfläche die Option **Anti-Spam**, und wählen Sie **Anti-Spam-Einstellungen**.

10. Wählen Sie im rechten Fensterbereich die Registerkarte **Scannen öffentlicher Ordner** aus, und aktivieren Sie die Option **Scannen öffentlicher Ordner**.

11. Geben Sie im Bereich **IMAP-Konfiguration** den IMAP-Server ein (Ihr Lotus Domino-Server, den Port und die Anmeldeinformationen des Benutzers, der auf den Ordner zugreifen soll).

> **HINWEIS**
>
> Die Test-Schaltfläche funktioniert hier nicht.

12. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern.



Screenshot 11: Scannen öffentlicher Ordner aktivieren

13. Ändern Sie in der Registrierung die Werte, um diese Funktion zu aktivieren. Wählen Sie in der Registrierung den Eintrag `HKEY_LOCAL_MACHINE\SOFTWARE\GFI\ME12\ATTENDANT\RPFOLDERS:5`, und legen Sie den folgenden Schlüsselwert an:

```
Name/Wert
SharedNamespace Public Folders\\Public Folder
FolderDelimiter \\
```

3.3 Installationsvorgang

In diesem Abschnitt wird beschrieben, wie Sie GFI MailEssentials installieren.

3.3.1 Wichtige Hinweise

1. Wenn Sie derzeit eine ältere Version von GFI MailEssentials verwenden, können Sie ein Upgrade Ihrer aktuellen Installation durchführen und so alle vorhandenen Konfigurationseinstellungen beibehalten. Ein Upgrade kann nicht rückgängig gemacht werden. Sie können also nicht zur vorher installierten Version zurückkehren.Weitere Informationen finden Sie unter „Aktualisieren von früheren Versionen“ (Seite 47).

2. Weitere Information zum Upgrade auf GFI MailEssentials von VIPRE Email Security for Exchange finden Sie unter http://go.gfi.com/?pageid=ME_VPXUpgrade

3. Wenn Sie einen Software-Wartungsvertrag besitzen, können Sie im Kundenbereich der GFI-Website ein Upgrade Ihres aktuellen Lizenzschlüssels durchführen.

HINWEIS

'Testversion' wird als Lizenzschlüssel nicht mehr akzeptiert. Führen Sie im Kundenbereich der GFI-Website ein Upgrade Ihres Lizenzschlüssels durch, bevor Sie mit dem Upgrade-Prozess beginnen.

4. Laden Sie das passende GFI MailEssentials-Build für Ihren Rechnertyp herunter. Verwenden Sie GFI MailEssentials 32 Bit (x86) für 32-Bit-Systeme und 64 Bit (x64) für 64-Bit-Systeme.

5. Bevor Sie den Installationsassistenten ausführen, stellen Sie Folgendes sicher:

» Sie sind mit einem Konto mit Administratorrechten angemeldet.

» Der Rechner, auf dem Sie GFI MailEssentials installieren möchten, erfüllt die angegebenen Systemanforderungen. Weitere Informationen finden Sie unter „Systemanforderungen“ (Seite 21).

» Konfigurieren Sie Ihre Firewall so, dass GFI MailEssentials eine Verbindung mit GFI-Servern herstellen darf. Weitere Informationen finden Sie unter „Firewall-Port-Einstellungen“ (Seite 24).

» Deaktivieren Sie das Scannen von Ordnern, die von GFI MailEssentials verwendet werden, durch Antiviren- und Backup-Software von Drittanbietern. Weitere Informationen finden Sie unter „Antiviren- und Backup-Software“ (Seite 23).

» Wenn Sie GFI MailEssentials auf einem E-Mail-Gateway- oder Relay-/Perimeter-Server installieren, konfigurieren Sie diesen Rechner so, dass er als Gateway agiert.Weitere Informationen finden Sie unter „Installation auf einem Mail-Gateway- oder Relay-/Perimeter-Server“ (Seite 25).

» Speichern Sie aktuelle Arbeiten, und schließen Sie alle auf dem Computer geöffneten Anwendungen.

6. Bei der Installation von GFI MailEssentials werden Microsoft® Exchange- oder Microsoft IIS® SMTP-Dienste neu gestartet. Dies ist erforderlich, damit die GFI MailEssentials-Komponenten ordnungsgemäß registriert werden können. Es wird empfohlen, GFI MailEssentials zu einem Zeitpunkt zu installieren, wo ein Neustart dieser Dienste Ihr Netzwerk am wenigsten beeinträchtigt.

3.3.2 Den Installations-Assistenten ausführen

1. Führen Sie das Setup-Programm für GFI MailEssentials aus.

2. Wählen Sie die Sprache für diese Installation von GFI MailEssentials und klicken Sie auf **Installieren**.

HINWEIS

Die Sprachauswahl kann nicht rückgängig gemacht werden. Das Ändern der hier ausgewählten Sprache ist nur durch eine Neuinstallation von GFI MailEssentials möglich.

3. Klicken Sie auf der Seite **Willkommen** auf **Weiter**.

4. Wählen Sie aus, ob nach neueren Versionen/Builds von GFI MailEssentials gesucht werden soll, und klicken Sie auf **Weiter**.

5. Lesen Sie die Lizenzvereinbarung, und klicken Sie auf **Ich stimme der Lizenzvereinbarung zu**, wenn Sie die Bedingungen akzeptieren. Klicken Sie auf **Weiter**.

GFI MailEssentials for Exchange/SMTP
E-Mail-Adresse des Administrators und Lizenzschlüssel
Geben Sie die E-Mail-Adresse des Administrators und den Lizenzschlüssel ein
GFI
Geben Sie die Administrator-E-Mail-Adresse ein.
E-Mail-Adresse des Administrators:
Administrator@domain.com
Geben Sie den Lizenzschlüssel für die Test- oder die registrierte Version von GFI MailEssentials for Exchange/SMTP ein.
Lizenzschlüssel:
< Zurück
Weiter >
Abbrechen

Screenshot 12: Angabe der E-Mail-Adresse des Administrators und des Lizenzschlüssels

6. Geben Sie die Administrator-E-Mail-Adresse im Bereich **E-Mail-Adresse des Administrators** ein, und geben Sie den **Lizenzschlüssel** ein. Klicken Sie auf **Weiter**.

> **HINWEIS**
>
> 'Testversion' wird als Lizenzschlüssel nicht mehr akzeptiert. Führen Sie im Kundenbereich der GFI-Website ein Upgrade Ihres Lizenzschlüssels durch, bevor Sie mit dem Upgrade-Prozess beginnen.

7. Wählen Sie den Modus, mit dem GFI MailEssentials die Liste der E-Mail-Benutzer abruft.

Option	Beschreibung
Ja, alle E-Mail-Benutzer sind in Active Directory verfügbar. Die Regeln richten sich nach den Active Directory-Benutzern.	**Active Directory-Modus** GFI MailEssentials ruft die Liste der Benutzer von Active Directory ab. Wenn Sie diese Option auswählen, wird GFI MailEssentials hinter Ihrer Firewall installiert und hat Zugriff auf das Active Directory, das ALLE Ihre E-Mail-Benutzer enthält.
Nein, ich verfüge nicht über Active Directory bzw. mein Netzwerk kann nicht auf Active Directory (DMZ) zugreifen.	**SMTP-Modus** Wählen Sie diesen Modus aus, wenn Sie GFI MailEssentials auf einem Rechner installieren, der keinen Zugriff auf das Active Directory mit der vollständigen Liste Ihrer E-Mail-Benutzer hat. Dazu zählen Rechner in einer DMZ oder Rechner, die nicht zur Active Directory-Domäne gehören. In diesem Modus füllt GFI MailEssentials die Liste der lokalen Benutzer automatisch mithilfe der Absenderadressen ausgehender E-Mails. Die Benutzerliste kann auch in den allgemeinen Einstellungen von GFI MailEssentials verwaltet werden. Weitere Informationen finden Sie unter „Verwalten lokaler Benutzer“ (Seite 249).

Klicken Sie auf **Weiter**.

GFI MailEssentials for Exchange/SMTP
Webserver-Setup
Website, auf der die Konfiguration und die virtuellen RSS-Verzeichnisse registriert werden.
GFI
GFI MailEssentials for Exchange/SMTP erfordert die Erstellung von zwei virtuellen Verzeichnissen für die Konfigurations-UI und den RSS-Zugriff. Wählen Sie die Namen für die virtuellen Verzeichnisse sowie die Website aus, auf der sie erstellt werden sollen.
IIS-Website
Default Web Site (http://serv801/)
Konfigurationspfad
MailEssentials
RSS-Pfad
MailEssentialsRSS
< Zurück
Weiter >
Abbrechen

Screenshot 13: Informationen zum SMTP-Server und virtuellen Verzeichnis

8. Konfigurieren Sie im Dialogfeld **Webserver-Setup** die folgenden Optionen:

> **HINWEIS**
>
> Die Standardeinstellungen sind für die meisten Installationen korrekt.

Option	Beschreibung
Die Website zum Erstellen des virtuellen Verzeichnisses von GFI MailEssentials	Wählen Sie die Website aus, auf der Sie die virtuellen Verzeichnisse von GFI MailEssentials hosten möchten.
Das virtuelle Verzeichnis für GFI MailEssentials Configuration	Geben Sie einen Namen für das virtuelle Verzeichnis von GFI MailEssentials an.
Das virtuelle Verzeichnis für Quarantäne-RSS-Feeds von GFI MailEssentials	Geben Sie einen Namen für das virtuelle Verzeichnis für Quarantäne-RSS-Feeds von GFI MailEssentials an.
SMTP-Server-Setup	Wählen Sie den SMTP-Server aus, an den GFI MailEssentials gebunden werden soll. Standardmäßig wird GFI MailEssentials an Ihren virtuellen Standardserver für SMTP gebunden. Wenn Ihre Domäne mehrere virtuelle SMTP-Server enthält, können Sie GFI MailEssentials an einen verfügbaren virtuellen SMTP-Server Ihrer Wahl binden. **NOTIZEN** 1. Bei Installation auf einem Rechner mit Microsoft® Exchange Server 2007/2010/2013 wird diese Option nicht angezeigt, da Microsoft® Exchange über einen eigenen integrierten SMTP-Server verfügt. 2. Sie können GFI MailEssentials auch nach der Installation an einen anderen virtuellen SMTP-Server binden. Dies erfolgt über GFI MailEssentials Configuration. Weitere Informationen finden Sie unter „Bindungen an virtuelle SMTP-Server“ (Seite 250).

Klicken Sie auf **Weiter**.

9. Wählen Sie den Ordner aus, in dem GFI MailEssentials installiert werden soll, und klicken Sie auf **Weiter**. Wenn es sich um ein Upgrade handelt, wird GFI MailEssentials am selben Speicherort wie bei der vorherigen Installation installiert.

10. Klicken Sie auf **Installieren**, um die Installation zu starten. Wenn Sie aufgefordert werden, die SMTP-Dienste neu zu starten, klicken Sie auf **Ja**.

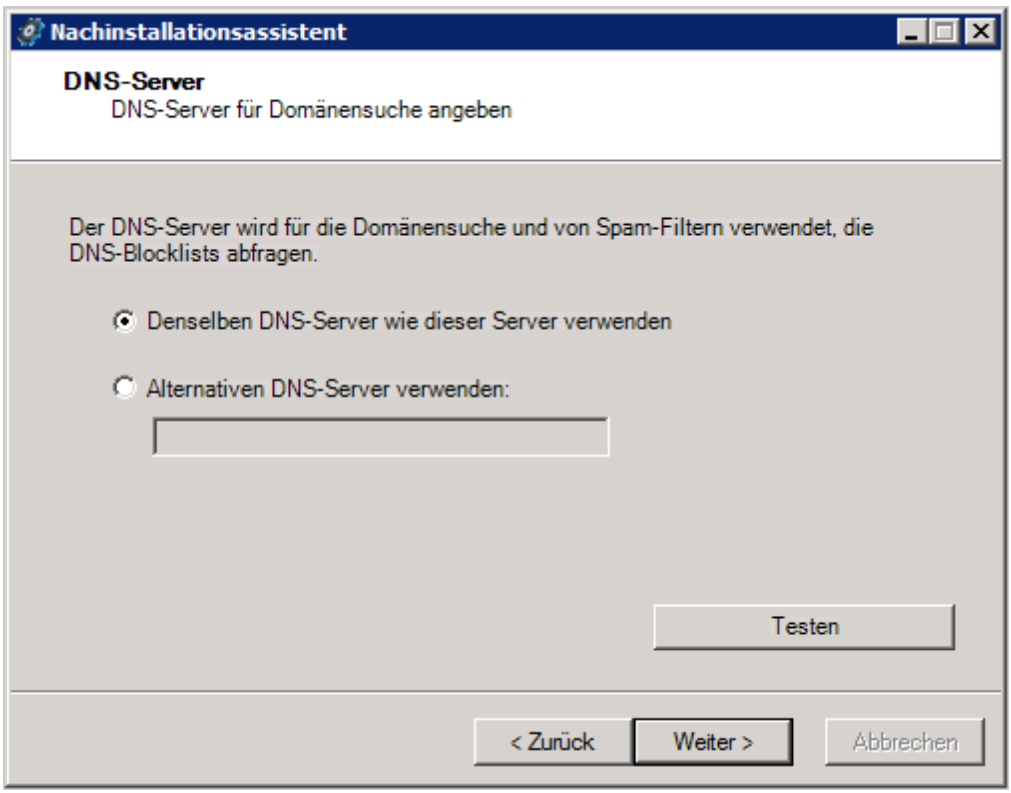
11. Klicken Sie nach Abschluss auf **Fertig stellen**.

> **HINWEIS**
>
> Bei neuen Installationen wird nun der Nachinstallationsassistent automatisch gestartet. Weitere Informationen finden Sie unter „Nachinstallationsassistent“ (Seite 43).

3.3.3 Nachinstallationsassistent

Der Nachinstallationsassistent wird automatisch geladen, nachdem GFI MailEssentials zum ersten Mal installiert wurde. Er ermöglicht die Konfiguration der wichtigsten Einstellungen von GFI MailEssentials.

1. Klicken Sie im Willkommensbildschirm auf **Weiter**.

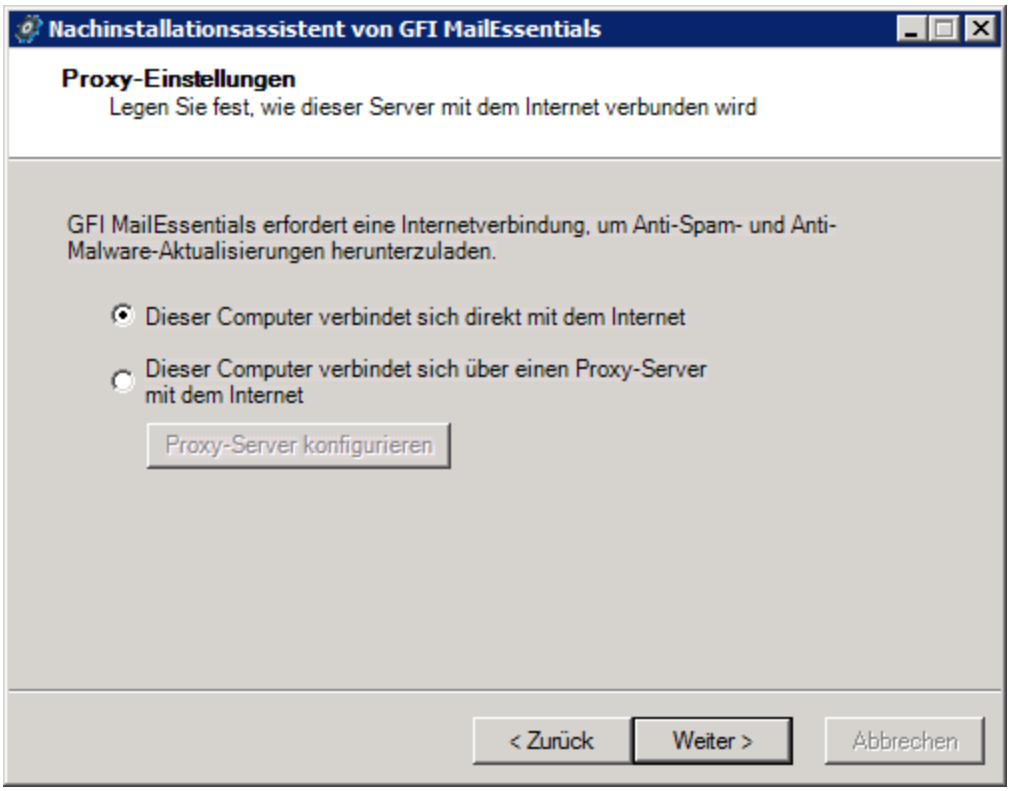


Screenshot 14: DNS-Servereinstellungen

2. Wählen Sie im DNS-Server-Dialogfeld Folgendes aus:

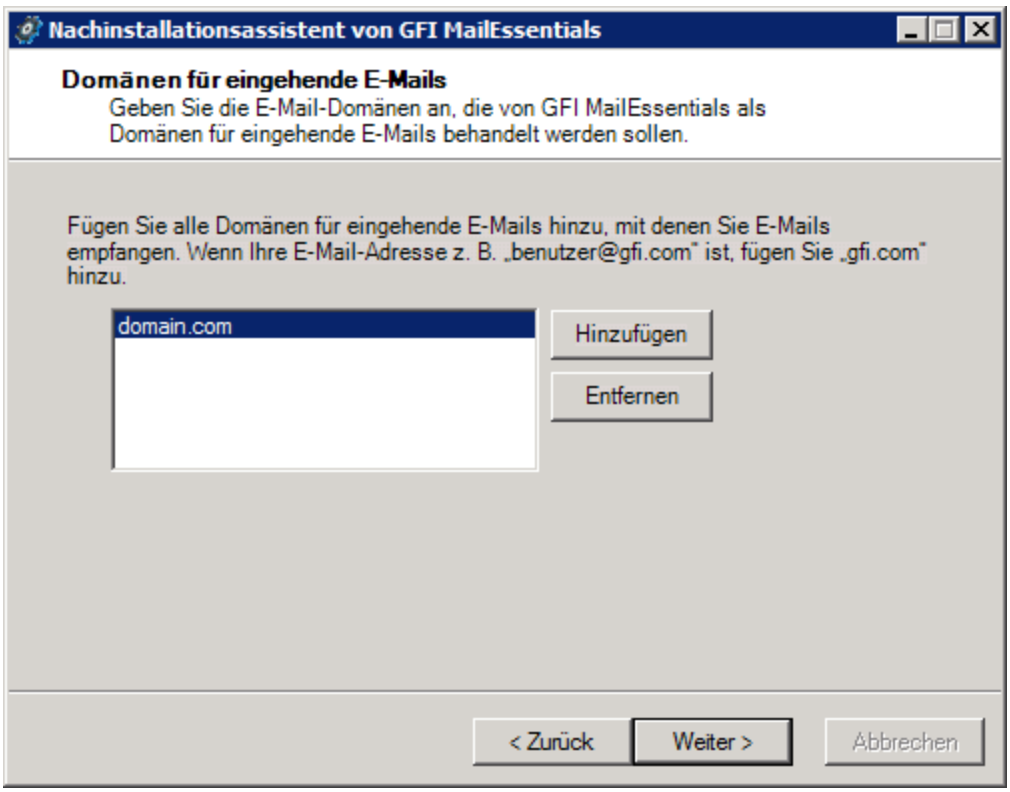
Option	Beschreibung
Den gleichen DNS-Server wie von diesem Server verwenden	Wählen Sie diese Option aus, um denselben DNS-Server wie das Betriebssystem zu verwenden, unter dem GFI MailEssentials installiert ist.
Alternativen DNS-Server verwenden	Wählen Sie diese Option aus, um eine benutzerdefinierte IP-Adresse für einen DNS-Server einzugeben.

Klicken Sie auf **Test**, um die Verbindung mit dem angegebenen DNS-Server zu testen. Falls der Test nicht erfolgreich ist, wählen Sie einen anderen DNS-Server. Klicken Sie auf **Weiter**.


Nachinstallationsassistent von GFI MailEssentials
Proxy-Einstellungen
Legen Sie fest, wie dieser Server mit dem Internet verbunden wird
GFI MailEssentials erfordert eine Internetverbindung, um Anti-Spam- und Anti-Malware-Aktualisierungen herunterzuladen.
Dieser Computer verbindet sich direkt mit dem Internet
Dieser Computer verbindet sich über einen Proxy-Server mit dem Internet
Proxy-Server konfigurieren
< Zurück
Weiter >
Abbrechen

Screenshot 15: Proxy-Einstellungen

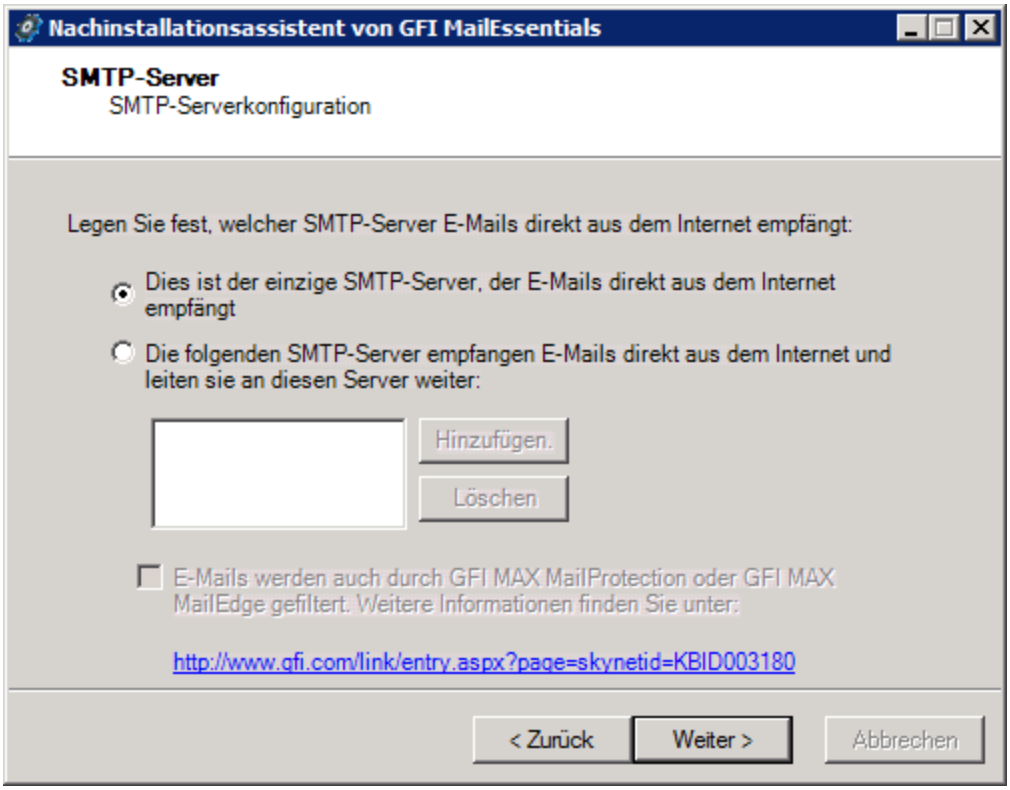
3. Legen Sie im Dialogfeld **Proxy-Einstellungen** fest, wie GFI MailEssentials eine Verbindung mit dem Internet herstellen soll. Wenn sich der Server über einen Proxy-Server verbindet, klicken Sie auf **Proxy-Server konfigurieren…**, und legen Sie die Proxy-Einstellungen fest. Klicken Sie auf **Weiter**.


Nachinstallationsassistent von GFI MailEssentials
Domänen für eingehende E-Mails
Geben Sie die E-Mail-Domänen an, die von GFI MailEssentials als Domänen für eingehende E-Mails behandelt werden sollen.
Fügen Sie alle Domänen für eingehende E-Mails hinzu, mit denen Sie E-Mails empfangen. Wenn Ihre E-Mail-Adresse z. B. „benutzer@gfi.com" ist, fügen Sie „gfi.com" hinzu.
domain.com
Hinzufügen
Entfernen
< Zurück
Weiter >
Abbrechen

Screenshot 16: Domänen für eingehende E-Mails

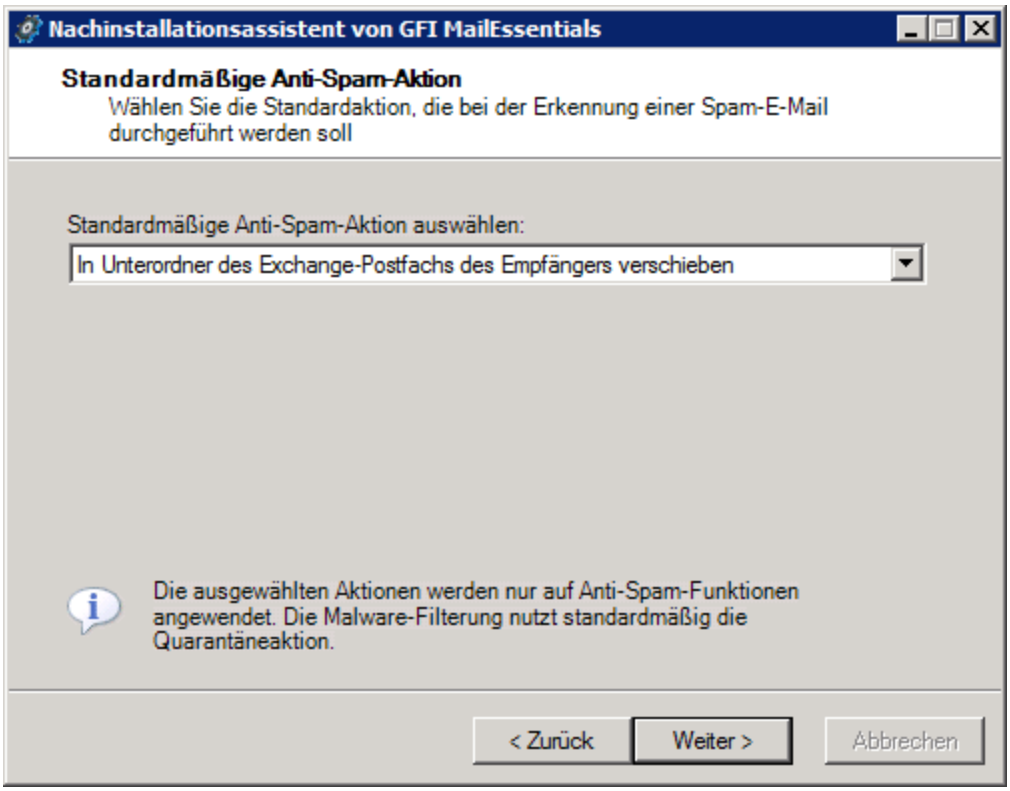
4. Geben Sie im Dialogfeld **Domänen für eingehende E-Mails** alle Domänen an, die auf Viren und Spam gescannt werden sollen. Lokale Domänen, die nicht in dieser Liste festgelegt werden, werden nicht gescannt. Klicken Sie auf **Weiter**.

> **HINWEIS**
>
> Wählen Sie beim Hinzufügen von Domänen die Option **MX-Einträge der Domäne abrufen und in die Liste der Perimeter-Server aufnehmen** aus, um die MX-Einträge der Domäne abzurufen und automatisch in die Liste der Perimeter-SMTP-Server (im nächsten Schritt konfiguriert) aufzunehmen.


Nachinstallationsassistent von GFI MailEssentials
SMTP-Server
SMTP-Serverkonfiguration
Legen Sie fest, welcher SMTP-Server E-Mails direkt aus dem Internet empfängt:
Dies ist der einzige SMTP-Server, der E-Mails direkt aus dem Internet empfängt
Die folgenden SMTP-Server empfangen E-Mails direkt aus dem Internet und leiten sie an diesen Server weiter:
Hinzufügen...
Löschen
E-Mails werden auch durch GFI MAX MailProtection oder GFI MAX MailEdge gefiltert. Weitere Informationen finden Sie unter:
http://www.gfi.com/link/entry.aspx?page=skynetid=KBID003180
< Zurück
Weiter >
Abbrechen

Screenshot 17: SMTP-Servereinstellungen

5. Geben Sie im Dialogfeld **SMTP-Server** an, wie der Server externe E-Mails empfängt. Wenn die E-Mails über andere Server geleitet werden, bevor sie an GFI MailEssentials übermittelt werden, fügen Sie die IP-Adressen dieser Server der Liste hinzu. Weitere Informationen zu Perimeter-SMTP-Servern finden Sie unter: http://go.gfi.com/?pageid=ME_PerimeterServer. Wenn Sie die gehosteten E-Mail-Sicherheitsprodukte GFI MAX MailProtection, GFI MAX MailEdge oder GFI MailEssentials Online verwenden, aktivieren Sie das Kontrollkästchen **E-Mails werden auch gefiltert von…**. Weitere Informationen finden Sie unter: http://go.gfi.com/?pageid=ME_MAXMPME. Klicken Sie auf **Weiter**.


Nachinstallationsassistent von GFI MailEssentials
Standardmäßige Anti-Spam-Aktion
Wählen Sie die Standardaktion, die bei der Erkennung einer Spam-E-Mail durchgeführt werden soll
Standardmäßige Anti-Spam-Aktion auswählen:
In Unterordner des Exchange-Postfachs des Empfängers verschieben
Die ausgewählten Aktionen werden nur auf Anti-Spam-Funktionen angewendet. Die Malware-Filterung nutzt standardmäßig die Quarantäneaktion.
< Zurück
Weiter >
Abbrechen

Screenshot 18: Auswahl der standardmäßigen Anti-Spam-Aktion

6. Wählen Sie im Dialogfeld **Standardmäßige Anti-Spam-Aktion** die Standardaktion aus, die beim Erkennen von Spam-E-Mails durchgeführt werden soll. Diese Aktion gilt nur für Anti-Spam-Filter. Malware-Filter verschieben blockierte E-Mails automatisch in die Quarantäne. Weitere Informationen finden Sie unter „Scan- und Filter-Engines für E-Mails“ (Seite 15).

> **HINWEIS**
>
> Wenn bei einer Installation auf Microsoft® Exchange 2010 die Standardaktion **In Unterordner des Exchange-Postfachs verschieben** ausgewählt wird, muss ein Benutzer mit Personifikationsrechten erstellt werden. Wählen Sie aus, ob GFI MailEssentials den Benutzer automatisch erstellen soll, oder legen Sie die Anmeldeinformationen manuell fest. Klicken Sie auf **Zugriffsrechte einstellen**, um dem angegebenen Benutzer die erforderlichen Rechte zuzuweisen. Dieser Benutzer darf nur für diese Funktion verwendet werden. Die Anmeldedaten dürfen nicht geändert werden. Weitere Informationen finden Sie unter http://go.gfi.com/?pageid=ME_SpamExch2010.

Klicken Sie auf **Weiter**.

7. Bei einer Installation auf Microsoft® Exchange Server 2007/2010 wird die Liste der Microsoft® Exchange-Serverrollen erkannt, und die erforderlichen GFI MailEssentials-Komponenten werden angezeigt. Klicken Sie auf **Weiter**, um die erforderlichen Komponenten von GFI MailEssentials zu installieren.

8. Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.

Die Installation von GFI MailEssentials ist nun abgeschlossen, und das E-Mail-Schutzsystem wird ausgeführt.

Nächster Schritt: Optimieren Sie Ihr Schutzsystem, um sicherzustellen, dass es effektiv arbeitet. Weitere Informationen finden Sie unter „Aktionen nach der Installation“ (Seite 49).

HINWEIS

Um den Nachinstallations-Assistenten erneut auszuführen, navigieren Sie in der Eingabeaufforderung zum Installationsordner von GFI MailEssentials, und führen Sie den folgenden Befehl aus:

```
e2kwiz.exe clean
```

3.4 Aktualisieren von früheren Versionen

Führen Sie ein Upgrade auf die neueste Version von GFI MailEssentials durch von:

» GFI MailEssentials 2012

» GFI MailEssentials 12 und höher und/oder GFI MailSecurity 10.1 und höher.

Wichtige Hinweise

1. Bevor Sie ein Upgrade auf die neueste Version von GFI MailEssentials durchführen, stellen Sie sicher, dass Ihr System die Mindestanforderungen erfüllt. Weitere Informationen finden Sie unter „Systemanforderungen“ (Seite 21).

2. Ein Upgrade kann nicht rückgängig gemacht werden. Sie können also nicht zur vorher installierten Version zurückkehren.

3.4.1 Upgrade von Version 2012 oder höher

Starten Sie für das Upgrade von GFI MailEssentials 2012 oder höher auf die neueste Version das neueste Installationsprogramm auf dem Server, auf dem GFI MailEssentials momentan installiert ist. Nachdem Sie die Endbenutzer-Lizenzvereinbarung akzeptiert haben, erkennt das Installationsprogramm die vorhandene Installation und zeigt den Installationspfad der früheren Version an. Klicken Sie auf **Weiter**, um das Upgrade durchzuführen, und zum Abschluss auf **Fertig stellen**.

Beim Upgrade von einer Hauptversion zu einer anderen ist ein neuer Lizenzschlüssel erforderlich, d. h. wenn Sie beispielsweise von GFI MailEssentials 2012 auf GFI MailEssentials 2014 upgraden. Erwerben Sie einen neuen Schlüssel im GFI-Kundenbereich.

Microsoft® Exchange 2007 oder höher

Bei Upgrades auf Microsoft® Exchange 2007 und höher wird nach der Installation der Nachinstallationsassistent angezeigt. Er zeigt nur die Liste der erkannten Microsoft® Exchange-Serverrollen und die erforderlichen GFI MailEssentials-Komponenten an. Klicken Sie auf **Weiter**, um die erforderlichen Komponenten von GFI MailEssentials zu installieren, und auf **Fertig stellen**, um den Nachinstallationsassistenten abzuschließen.

3.4.2 Upgrade von älteren Versionen

Information zum Upgrade auf die neueste Version von GFI MailEssentials von:

» GFI MailEssentials-Versionen 12, 14, 2010

» GFI MailSecurity-Versionen 10.1 und 2011

In GFI MailEssentials 2012 und 2014 fanden einige Veränderungen der verfügbaren Funktionen für die obigen Versionen statt. Weitere Informationen finden Sie in unter GFI MailEssentialsUpgrade-Handbuch. Wichtigste Änderungen:

- Anti-Spam- und Anti-Virus-Funktionen wurden in einer Lösung zusammengefasst
- Neue webbasierte Benutzeroberfläche
- Unterschiedliche, verfügbare Anti-Virus-Engines
- Die Berichterstellung ist in die Benutzeroberfläche integriert
- Weitere Aktualisierungen

Wählen Sie die Umgebung, in der Sie das Upgrade durchführen:

- GFI MailEssentials-Versionen 12, 14, 2010
- GFI MailSecurity-Versionen 10.1 und 2011
- Sowohl GFI MailEssentials als auch GFI MailSecurity

Upgrade unter GFI MailEssentials-Versionen 12, 14, 2010

Anti-Spam- und Anti-Phishing-Funktionen werden beim Upgrade lizenziert. Die Anti-Virus- und Anti-Malware-Funktionen werden als 30-tägige Testversion bereitgestellt.

Installieren Sie GFI MailEssentials wie bei einer Erstinstallation. Weitere Informationen finden Sie unter „Installationsvorgang“ (Seite 39).

Bei Upgrades auf Microsoft® Exchange 2007 und höher wird nach der Installation der Nachinstallationsassistent angezeigt. Er zeigt nur die Liste der erkannten Microsoft® Exchange-Serverrollen und die erforderlichen GFI MailEssentials-Komponenten an. Klicken Sie auf **Weiter**, um die erforderlichen Komponenten von GFI MailEssentials zu installieren, und auf **Fertig stellen**, um den Nachinstallationsassistenten abzuschließen.

Upgrade unter GFI MailSecurity-Versionen 10.1 und 2011

Anti-Virus- und Anti-Malware-Funktionen werden beim Upgrade lizenziert. Die Anti-Spam- und Anti-Phishing-Funktionen werden als 30-tägige Testversion bereitgestellt.

Installieren Sie GFI MailEssentials wie bei einer Erstinstallation. Weitere Informationen finden Sie unter „Installationsvorgang“ (Seite 39).

Führen Sie nach der Installation auch den Nachinstallationsassistenten von GFI MailEssentials aus. Weitere Informationen finden Sie unter „Nachinstallationsassistent“ (Seite 43).

Upgrade unter GFI MailEssentials und GFI MailSecurity

Beim Upgrade auf einem Server, auf dem sowohl GFI MailEssentials als auch GFI MailSecurity installiert ist, werden alle Anti-Virus-, Anti-Malware-, Anti-Spam- und Anti-Phishing-Funktionen beim Upgrade lizenziert.

Installieren Sie GFI MailEssentials wie bei einer Erstinstallation. Weitere Informationen finden Sie unter „Installationsvorgang“ (Seite 39).

Bei Upgrades auf Microsoft® Exchange 2007 und höher wird nach der Installation der Nachinstallationsassistent angezeigt. Er zeigt nur die Liste der erkannten Microsoft® Exchange-Serverrollen und die erforderlichen GFI MailEssentials-Komponenten an. Klicken Sie auf **Weiter**, um die erforderlichen Komponenten von GFI MailEssentials zu installieren, und auf **Fertig stellen**, um den Nachinstallationsassistenten abzuschließen.

3.5 Aktionen nach der Installation

Führen Sie nach der Installation die folgenden Aktionen aus, um sicherzustellen, dass das Scan- und Filtersystem von GFI MailEssentials effektiv arbeitet:

Aktion	Beschreibung
Scan-Engines von GFI MailEssentials zur Windows DEP-Ausnahmenliste hinzufügen	Die Datenausführungsverhinderung (DEP) ist eine Kombination aus Hardware- und Softwaretechnologien, die Speicherüberprüfungen durchführen, um die Ausführung von schädlichem Code auf dem System zu verhindern. Wenn Sie GFI MailEssentials auf einem Betriebssystem mit DEP installiert haben, müssen Sie die ausführbaren Dateien der GFI MailEssentials-Scan-Engine (**GFiScanM.exe**) und der Virenscan-Engine von Kaspersky (**kavss.exe**) hinzufügen. **HINWEIS** Dies ist nur bei einer Installation auf Microsoft® Windows Server 2003 SP1 oder SP2 erforderlich. Weitere Informationen finden Sie unter „Hinzufügen von Engines zur Windows DEP-Ausnahmenliste“ (Seite 49).
GFI MailEssentials Configuration starten	Wählen Sie **Start > Programme > GFI MailEssentials > GFI MailEssentials Configuration** aus.
Directory Harvesting aktivieren	Directory Harvesting-Angriffe treten auf, wenn Spammer versuchen, E-Mail-Adressen zu erraten, indem sie Ihrer Domäne bekannte Benutzernamen hinzufügen. Die Mehrheit der E-Mail-Adressen existiert nicht. Dieser Filter wird bei der Installation von GFI MailEssentials in einer Active Directory-Umgebung standardmäßig aktiviert. Weitere Informationen finden Sie unter „Directory Harvesting“ (Seite 117).
Greylist aktivieren	Der Greylist-Filter blockiert temporär eingehende E-Mails von unbekannten Absendern. Zulässige Mailsysteme versuchen normalerweise, die E-Mail nach einigen Minuten erneut zu senden, Spammer hingegen ignorieren solche Fehlernachrichten einfach. Dieser Filter ist nicht standardmäßig aktiviert. Weitere Informationen finden Sie unter „Greylist“ (Seite 132).Weitere Informationen finden Sie unter „Greylist“ (Seite 132).
Whitelists konfigurieren	Die Whitelist enthält Listen von Kriterien, die zulässige E-Mails identifizieren. E-Mails, die diesen Kriterien entsprechen, werden nicht von Anti-Spam-Filtern geprüft und immer direkt dem Empfänger zugestellt. Weitere Informationen finden Sie unter „Whitelist“ (Seite 142).
Testen Ihrer Installation	Nachdem Sie alle Aktionen nach der Installation konfiguriert haben, ist GFI MailEssentials einsatzbereit und kann Ihr Mailsystem vor schädlichen E-Mails und Spam schützen. Testen Sie Ihre Installation, um sicherzustellen, dass GFI MailEssentials ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter „Testen Ihrer Installation“ (Seite 50).

3.5.1 Hinzufügen von Engines zur Windows DEP-Ausnahmenliste

Die Datenausführungsverhinderung (DEP) ist eine Kombination aus Hardware- und Softwaretechnologien, die Speicherüberprüfungen durchführen, um die Ausführung von schädlichem Code auf dem System zu verhindern.

Wenn Sie GFI MailEssentials auf einem Betriebssystem mit DEP installiert haben, müssen Sie die ausführbaren Dateien der GFI MailEssentials-Scan-Engine (**GFiScanM.exe**) und der Virenscan-Engine von Kaspersky (**kavss.exe**) hinzufügen.

> **HINWEIS**
>
> Dies ist nur bei einer Installation auf Microsoft® Windows Server 2003 SP1 oder SP2 erforderlich.

So fügen Sie ausführbare Dateien von GFI zur Ausnahmenliste der Datenausführungsverhinderung hinzu:

1. Öffnen Sie in der **Systemsteuerung** die Option **System**.

2. Klicken Sie auf der Registerkarte **Erweitert** im Bereich **Leistung** auf **Einstellungen**.

3. Klicken Sie auf die Registerkarte **Datenausführungsverhinderung**.

4. Klicken Sie auf **Datenausführungsverhinderung für alle Programme und Dienste mit Ausnahme der ausgewählten einschalten**.

5. Klicken Sie auf **Hinzufügen**, navigieren Sie im Dialogfeld zu **<*GFI MailEssentials Installationspfad*>*GFI**MailEssentials*\EmailSecurity**, und wählen Sie **GFiScanM.exe** aus.

6. Klicken Sie auf **Hinzufügen**, navigieren Sie im Dialogfeld zu **<*GFI MailEssentials Installationspfad*>*GFI**MailEssentials*\AntiVirus\Kaspersky**, und wählen Sie **kavss.exe** aus.

7. Klicken Sie auf **Übernehmen** und **OK**, um die Änderungen zu übernehmen.

8. Starten Sie den **GFI MailEssentials Autoupdater**-Dienst und die **GFI MailEssentials AV-Scan-Engine**-Dienste neu.

3.5.2 Testen Ihrer Installation

Nachdem Sie alle Aktionen nach der Installation konfiguriert haben, ist GFI MailEssentials einsatzbereit und kann Ihr Mailsystem vor schädlichen E-Mails und Spam schützen.

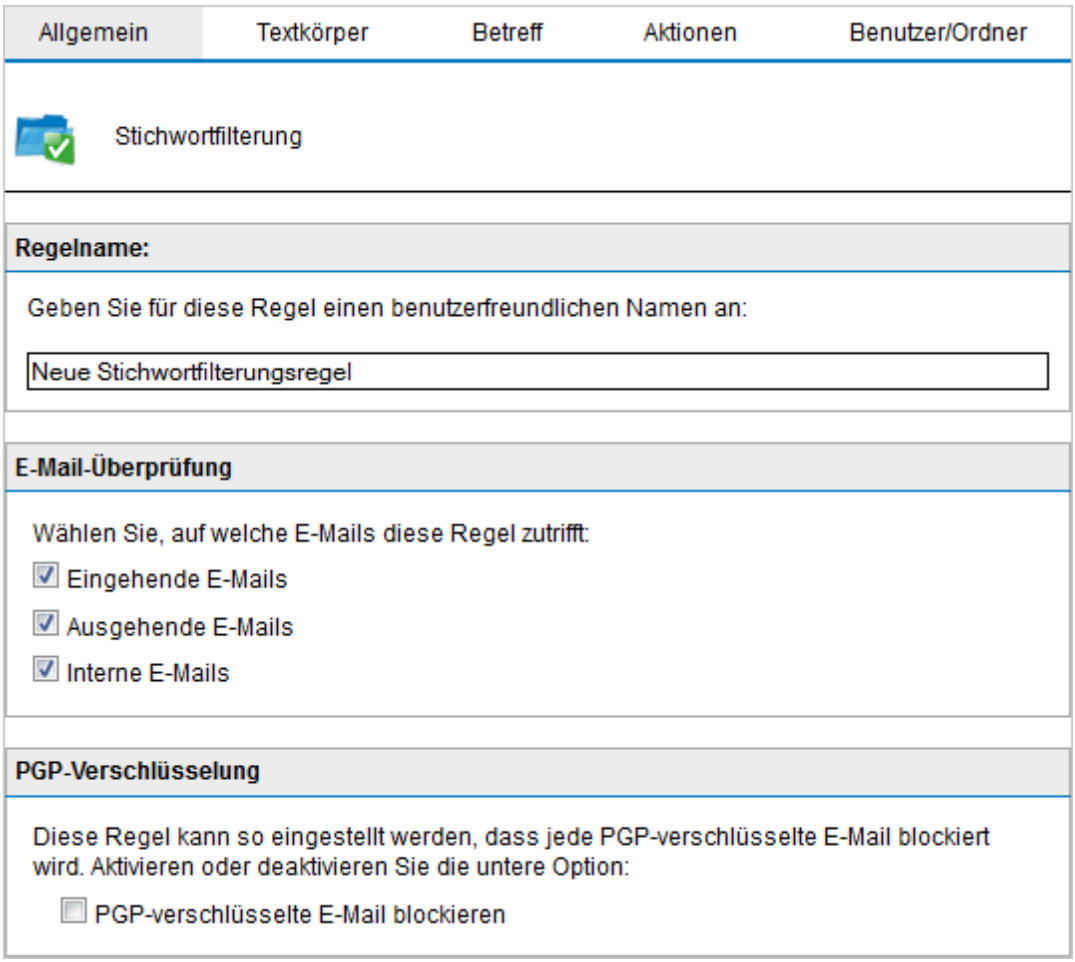
Stellen Sie sicher, dass GFI MailEssentials unerwünschte E-Mails blockiert. Senden Sie dazu eingehende und ausgehende Test-E-Mails, die bewusst so aufgebaut sind, dass sie von GFI MailEssentials blockiert werden.

Schritt 1: Erstellen einer Regel für die Inhaltsfilterung

1. Starten Sie die GFI MailEssentials-Konsole.

2. Wählen Sie **GFI MailEssentialsInhaltsfilterung > Stichwortfilterung** aus.

3. Klicken Sie auf **Regel hinzufügen...**.



Screenshot 19: Erstellen einer Testregel für die Stichwortfilterung

4. Geben Sie unter **Regelname** den Namen `Testregel` ein.

5. Wählen Sie in der Registerkarte **Betreff** die Option **E-Mails blockieren, wenn der Inhalt (Nachrichtenbetreff) diese Bedingungen erfüllt**.

6. Geben Sie unter **Bedingung bearbeiten** den Text `Test auf Bedrohungen` ein, und klicken Sie auf **Bedingung hinzufügen**.

7. Aktivieren Sie auf der Registerkarte **Aktionen** die Option **E-Mail blockieren und diese Aktion durchführen**, und wählen Sie **E-Mail in Quarantäne verschieben** aus.

8. Klicken Sie auf **Übernehmen**, um die Regel zu speichern.

Schritt 2: Senden einer eingehenden Test-E-Mail

1. Erstellen Sie mit einem externen E-Mail-Konto eine neue E-Mail mit dem Betreff `Test auf Bedrohungen`.

2. Senden Sie die E-Mail an eine Ihrer internen E-Mail-Adressen.

Schritt 3: Senden einer ausgehenden Test-E-Mail

1. Erstellen Sie mit einem internen E-Mail-Konto eine neue E-Mail mit dem Betreff `Test auf Bedrohungen`.

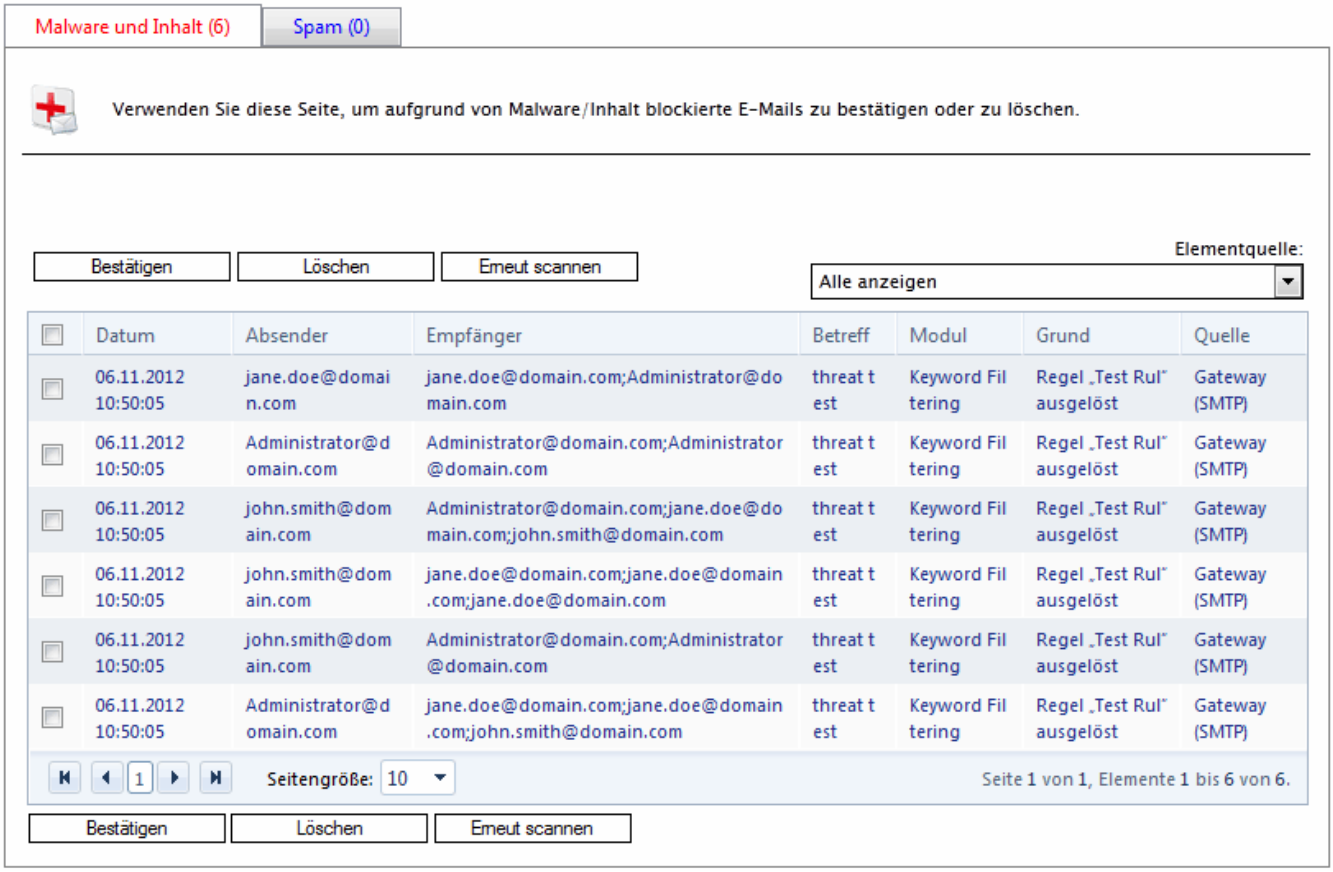
2. Senden Sie die E-Mail an eine externe E-Mail-Adresse.

Schritt 4: Prüfen, ob die Test-E-Mails blockiert wurden

Überprüfen Sie, ob die eingehende und die ausgehende Test-E-Mail blockiert und in die Quarantäne verschoben wurden. Gehen Sie dazu wie folgt vor:

1. Wählen Sie in GFI MailEssentials die Optionen **GFI MailEssentials Konfiguration > Quarantäne > Heute** aus.

2. Überprüfen Sie, ob die eingehende und die ausgehende Test-E-Mail auf der Registerkarte **Malware und Inhalt** aufgelistet sind, und zwar mit folgender Begründung: **Regel „Testregel“ ausgelöst**.



Screenshot 20: Durch Testregel blockierte Test-E-Mails

HINWEIS

Wenn der Test erfolgreich abschlossen wurde, löschen oder deaktivieren Sie die in Schritt 1 erstellte **Testregel**.

4 Statusüberwachung

GFI MailEssentials ermöglicht die Überwachung Ihrer E-Mail-Aktivitäten in Echtzeit oder durch das Erstellen von Berichten für einen bestimmten Zeitraum.

Überwachungsmodul	Beschreibung
Dashboard	Das GFI MailEssentials-**Dashboard** stellt Echtzeit-Informationen zur Überwachung des Produkts zur Verfügung. Zum Öffnen des Dashboards wählen Sie **GFI MailEssentials > Dashboard** aus. Folgende Informationen sind verfügbar: » Wichtige statistische Informationen über blockierte E-Mails. Weitere Informationen finden Sie unter „Status und Statistiken“ (Seite 54). » Status der GFI MailEssentials-Dienste. Weitere Informationen finden Sie unter „Dienste“ (Seite 55). » Grafische Darstellung der E-Mail-Aktivitäten. Weitere Informationen finden Sie unter „Diagramme“ (Seite 56). » Liste der verarbeiteten E-Mails. Weitere Informationen finden Sie unter „E-Mail-Verarbeitungsprotokolle“ (Seite 57). » Status der Softwareaktualisierungen. Weitere Informationen finden Sie unter „Aktualisierungen der Anti-Virus- und Anti-Spam-Engines“ (Seite 59). » Aufzeichnung wichtiger GFI MailEssentials-Ereignisse. Weitere Informationen finden Sie unter „Ereignisprotokolle“ (Seite 60). » Protokoll der POP2Exchange-Aktivitäten. Weitere Informationen finden Sie unter „POP2Exchange-Aktivitäten“ (Seite 61).
Berichte	GFI MailEssentials ermöglicht das Erstellen von Berichten basierend auf Daten, die in einer Datenbank protokolliert sind. Zum Öffnen der Berichterstellung wählen Sie **GFI MailEssentials > Berichterstellung** aus. » **Aktivieren der Berichterstellung** - Weitere Informationen finden Sie unter „Aktivieren/Deaktivieren der Berichterstellung“ (Seite 61). » **Konfigurieren der Berichtsdatenbank** - Weitere Informationen finden Sie unter „Konfigurieren der Berichtsdatenbank“ (Seite 68). » **Erstellen eines Berichts** - Weitere Informationen finden Sie unter „Erstellen eines Berichts“ (Seite 62). » **Erstellen Sie benutzerdefinierte Berichte**: Weitere Informationen finden Sie unter „Benutzerdefinierte Berichte“ (Seite 65). » **Durchsuchen der Berichtsdatenbank** - Weitere Informationen finden Sie unter „Durchsuchen der Berichtsdatenbank“ (Seite 66).

4.1 Dashboard

Das GFI MailEssentials-**Dashboard** stellt Echtzeit-Informationen zur Überwachung des Produkts zur Verfügung. Zum Öffnen des Dashboards wählen Sie **GFI MailEssentials > Dashboard** aus. Folgende Informationen sind verfügbar:

» Wichtige statistische Informationen über blockierte E-Mails. Weitere Informationen finden Sie unter „Status und Statistiken“ (Seite 54).

» Status der GFI MailEssentials-Dienste. Weitere Informationen finden Sie unter „Dienste“ (Seite 55).

» Grafische Darstellung der E-Mail-Aktivitäten. Weitere Informationen finden Sie unter „Diagramme“ (Seite 56).

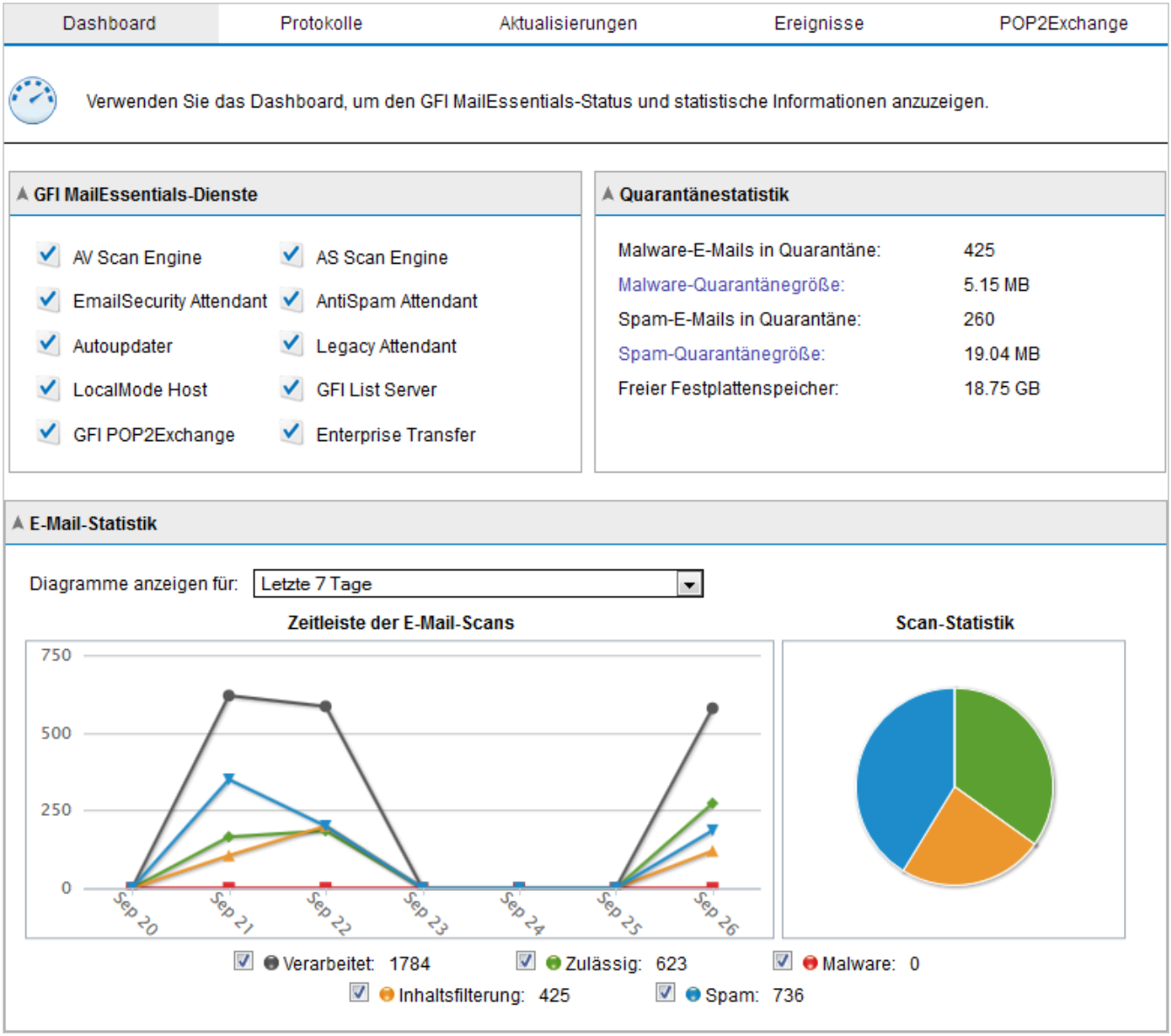
» Liste der verarbeiteten E-Mails. Weitere Informationen finden Sie unter „E-Mail-Verarbeitungsprotokolle“ (Seite 57).

» Status der Softwareaktualisierungen. Weitere Informationen finden Sie unter „Aktualisierungen der Anti-Virus- und Anti-Spam-Engines“ (Seite 59).

» Aufzeichnung wichtiger GFI MailEssentials-Ereignisse. Weitere Informationen finden Sie unter „Ereignisprotokolle“ (Seite 60).

» Protokoll der POP2Exchange-Aktivitäten. Weitere Informationen finden Sie unter „POP2Exchange-Aktivitäten“ (Seite 61).

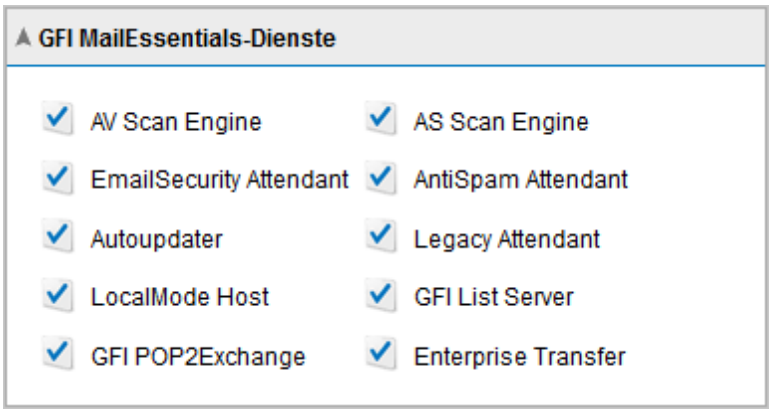
4.1.1 Status und Statistiken



Screenshot 21: Das GFI MailEssentials Dashboard

Zum Öffnen des Dashboards wählen Sie **GFI MailEssentials > Dashboard** aus. Auf dieser Seite werden Statistiken, der Status von Diensten und eine grafische Darstellung der E-Mail-Aktivitäten angezeigt. Die einzelnen Bereiche werden im Folgenden näher erläutert.

Dienste



Screenshot 22: Die GFI MailEssentials-Dienste

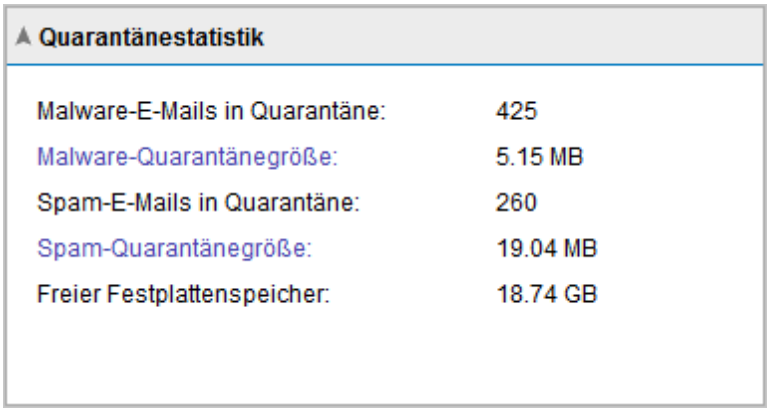
Der Bereich **Dienste** zeigt den Status der GFI MailEssentials-Dienste.

» - Gibt an, dass der Dienst gestartet wurde. Klicken Sie auf dieses Symbol, um den Dienst zu beenden.

» - Gibt an, dass der Dienst beendet wurde. Klicken Sie auf dieses Symbol, um den beendeten Dienst zu starten.

Sie können Dienste auch über die Konsole der Microsoft® Windows-Dienste starten oder beenden. Wählen Sie zum Starten der Dienste-Konsole **Start > Ausführen** aus, geben Sie `services.msc` ein, und klicken Sie auf **OK**.

Quarantänestatistik



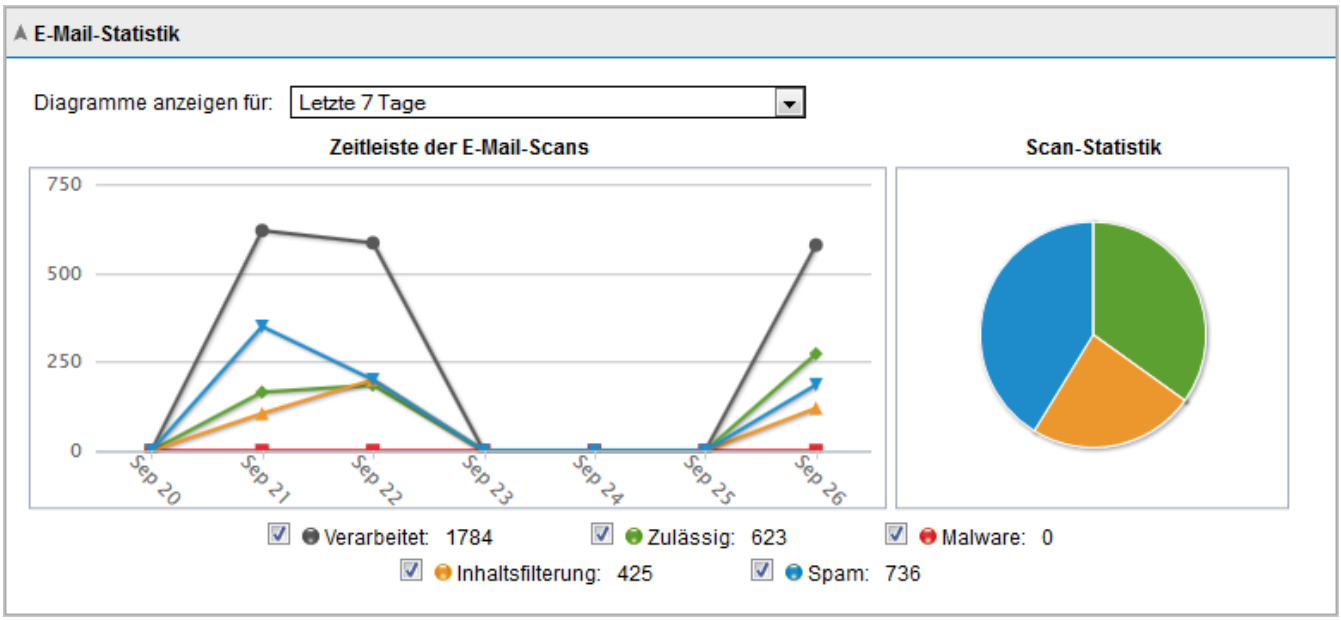
Screenshot 23: Quarantänestatistik

Im Bereich **Quarantänestatistik** werden die folgenden statistischen Informationen angezeigt:

Titel der Statistik	Beschreibung
Malware-E-Mails in Quarantäne	Die Anzahl der E-Mails, die von den Engines für E-Mail-Sicherheit und Inhaltsfilterung blockiert und in den Malware-Quarantänespeicher gestellt wurden.
Malware-Quarantänegröße	Die Datenbankgröße des Malware-Quarantänespeichers auf der Festplatte.
Spam-E-Mails in Quarantäne	Die Anzahl der E-Mails, die von den Anti-Spam-Engines blockiert und in den Spam-Quarantänespeicher gestellt wurden.

Titel der Statistik	Beschreibung
Spam-Quarantänegröße	Die Datenbankgröße des Spam-Quarantänespeichers auf der Festplatte.
Freier Festplattenspeicher	Freier Speicher auf der Festplatte, auf der sich die Quarantänespeicher befinden.

Diagramme

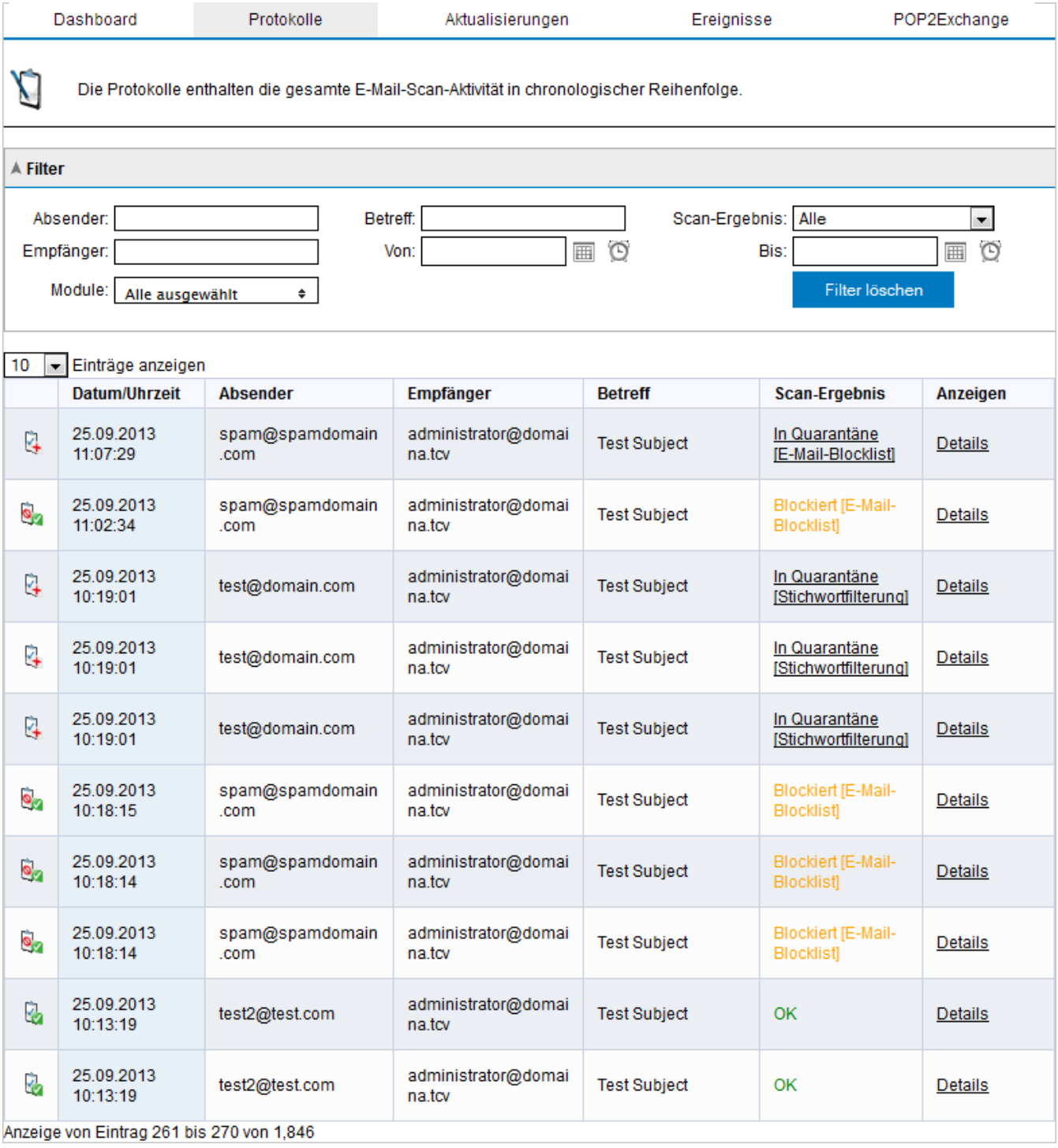


Screenshot 24: Dashboard-Diagramme

Im Bereich **Diagramme** werden Informationen zu den in GFI MailEssentials verarbeiteten E-Mails grafisch dargestellt. Wählen Sie in der Dropdown-Liste den Zeitraum aus, für den Sie Informationen anzeigen möchten.

Bereich	Beschreibung
Diagramme anzeigen für	Wählen Sie einen Zeitraum aus, für den Diagramme angezeigt werden sollen. Folgende Optionen sind verfügbar: » Letzte 6 Stunden » Letzte 24 Stunden » Letzte 48 Stunden » Letzte 7 Tage
Zeitleiste der E-Mail-Scans (Zeitdiagramm)	Zeigt ein Zeitdiagramm für den ausgewählten Zeitraum. Das Diagramm zeigt die Anzahl der verarbeiteten, zulässigen, nach Inhalten gefilterten und Spam-E-Mails.
Scan-Statistik (Kreisdiagramm)	Stellt die Gesamtanzahl der sicheren, in Quarantäne gestellten und fehlgeschlagenen E-Mails für den ausgewählten Zeitraum grafisch dar.
Legende	Die Legende zeigt die in den Diagrammen verwendeten Farben und die Anzahl der Elemente in jeder Kategorie.

4.1.2 E-Mail-Verarbeitungsprotokolle



Screenshot 25: E-Mail-Verarbeitungsprotokolle

In GFI MailEssentials Configuration können Sie alle verarbeiteten E-Mails in Echtzeit überwachen. Öffnen Sie **GFI MailEssentials > Dashboard**, und wählen Sie die Registerkarte **Protokolle** aus, um die Liste der verarbeiteten E-Mails anzuzeigen. Zu jeder verarbeiteten E-Mail werden folgende Details angezeigt:

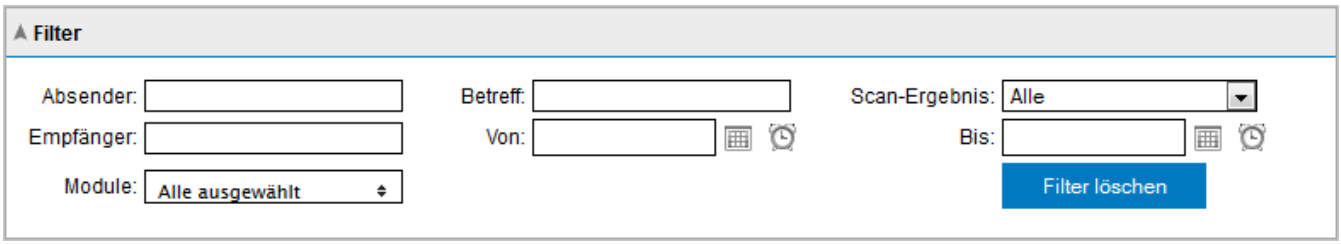
- Datum/Uhrzeit
- Absender
- Empfänger

» Betreff

» Scan-Ergebnisse – Zeigt, welche Aktion für die E-Mail durchgeführt wurde.

Aktion	Beschreibung
OK	Die E-Mail wurde nicht von GFI MailEssentials blockiert und wurde an den Empfänger zugestellt.
In Quarantäne	Die E-Mail wurde von einer Engine oder einem Filter blockiert, bei dem als Aktion das Verschieben in die Quarantäne eingestellt ist. Klicken Sie auf **Quarantäne**, um die E-Mail zu überprüfen. **HINWEIS** Die E-Mail kann in der Quarantäne nicht überprüft werden, wenn sie manuell aus der Quarantäne gelöscht wurde.
Blockiert	Die E-Mail wurde von einer Engine oder einem Filter blockiert. Es wurde die Aktion ausgeführt, die für die entsprechende Engine konfiguriert ist.
Gelöscht	Die E-Mail wurde von einer Engine oder einem Filter blockiert, bei dem als Aktion das Löschen der erkannten E-Mail eingestellt ist.
Fehlgeschlagen	Die E-Mail konnte nicht von GFI MailEssentials gescannt werden. Sie wurde in einen der folgenden Ordner verschoben: *<GFI MailEssentials Installationspfad>*\GFI\MailEssentials\EmailSecurity\FailedMails\ *<GFI MailEssentials Installationspfad>*\GFI\MailEssentials\AntiSpam\FailedMails\ Weitere Informationen finden Sie unter „Fehlgeschlagene E-Mails“ (Seite 259).

Filtern der E-Mail-Verarbeitungsprotokolle



Screenshot 26: Filter für E-Mail-Verarbeitungsprotokolle

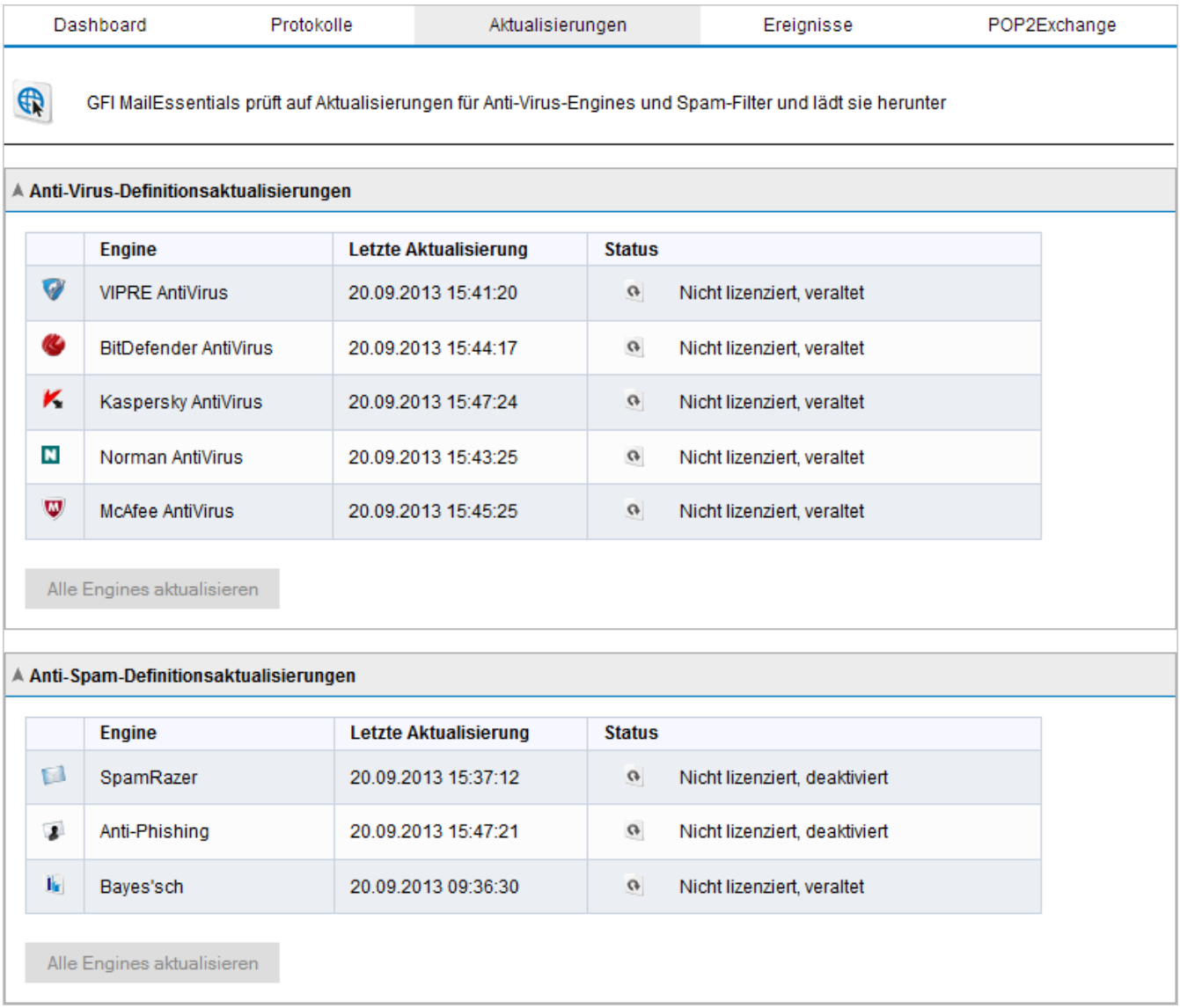
Durch das Filtern der E-Mail-Verarbeitungsprotokolle wird die Überprüfung vereinfacht, da gezielt nach bestimmten E-Mails gesucht werden kann. Geben Sie im Bereich **Filter** nach Bedarf die folgenden Kriterien an:

Filter	Beschreibung
Absender	Geben Sie eine E-Mail-Adresse vollständig oder teilweise an, um nur E-Mails von übereinstimmenden Absendern anzuzeigen.
Empfänger	Geben Sie eine E-Mail-Adresse vollständig oder teilweise an, um nur E-Mails an übereinstimmende Empfänger anzuzeigen.
Betreff	Geben Sie einen E-Mail-Betreff vollständig oder teilweise an, um nur E-Mails mit übereinstimmendem Betreff anzuzeigen.
Scan-Ergebnis	Wählen Sie in der Dropdown-Liste aus, ob nur E-Mails mit einem bestimmten Scan-Ergebnis angezeigt werden sollen (z. B. nur E-Mails in der Quarantäne).
Von/Bis	Geben Sie eine Datums- und Zeitspanne an, um E-Mails anzuzeigen, die innerhalb dieser Spanne verarbeitet wurden.

HINWEIS

Klicken Sie auf **Filter löschen**, um die festgelegten Filter zu löschen und alle E-Mail-Protokolle anzuzeigen.

4.1.3 Aktualisierungen der Anti-Virus- und Anti-Spam-Engines



Screenshot 27: Aktualisierungen für Virenscan-Engines

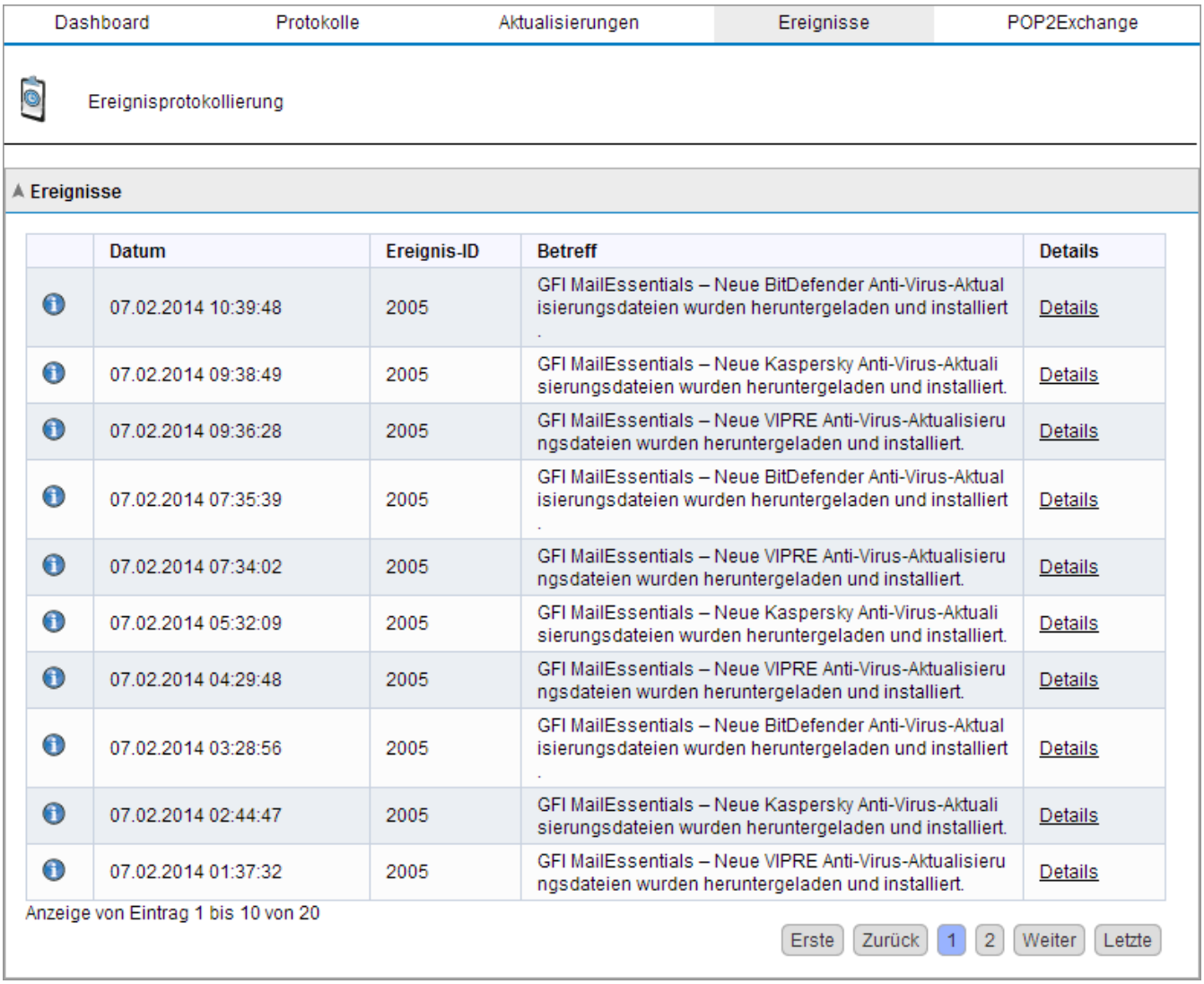
Die Aktualisierungen der Anti-Virus- und Anti-Spam-Engines können auf einer zentralen Seite überwacht werden. Öffnen Sie **GFI MailEssentials > Dashboard**, und wählen Sie die Registerkarte **Aktualisierungen** aus, um den Status und das Datum der letzten Aktualisierungen für die Scan-Engines anzuzeigen.

Klicken Sie auf **Alle Engines aktualisieren**, um auf Aktualisierungen zu prüfen und diese herunterzuladen.

Die Prüfung auf Aktualisierungen und das Herunterladen erfolgen jeweils so, wie dies auf den Konfigurationsseiten der Engines festgelegt wurde. Öffnen Sie die Konfigurationsseite einer Engine, um auf der Registerkarte **Aktualisierungen** die Einstellungen für diese Engine zu konfigurieren.

> **HINWEIS**
>
> Die Prüfung auf Aktualisierungen und das Herunterladen für die einzelnen Engines verlaufen sequenziell (eine Engine-Aktualisierung nach der anderen).

4.1.4 Ereignisprotokolle



Screenshot 28: Ereignisprotokolle

In der GFI MailEssentials-Konfiguration können Sie wichtige Ereignisse hinsichtlich der Funktionalität von GFI MailEssentials überwachen. Beispiele für Instanzen, die Ereignisse auslösen:

» Abschluss von Aktualisierungen der Anti-Spam-Engines

» Berichtsdatenbank erreicht 1,7 GB und GFI MailEssentials wechselt zu einer neuen Datenbank

» Weniger als 1 GB freier Festplattenspeicherplatz auf der Partition, wo sich die Quarantäne befindet

Öffnen Sie **GFI MailEssentials > Dashboard**, und wählen Sie die Registerkarte **Ereignisse**, um die Liste der Ereignisse anzuzeigen. Für jedes Ereignis werden folgende Informationen angezeigt:

» Datum/Uhrzeit

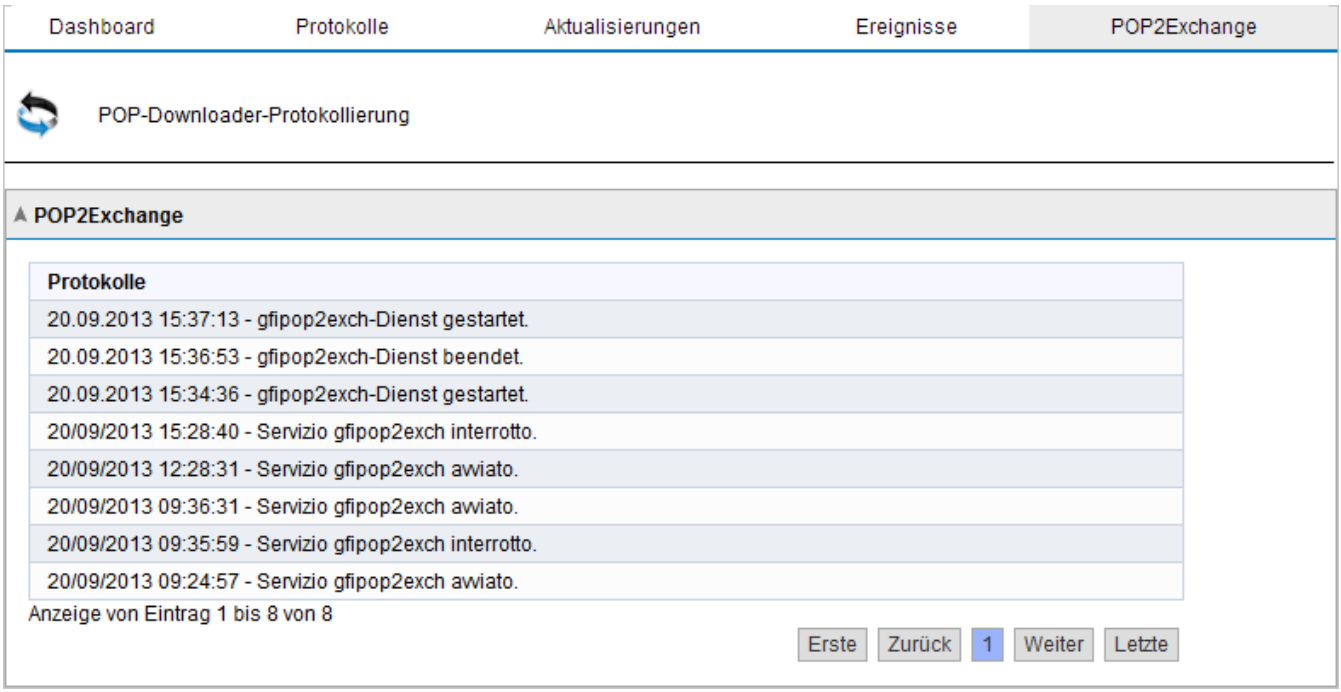
» Ereignis-ID – Jedem Typ eines GFI MailEssentials-Ereignisses wird eine Kennung zugewiesen.

» Betreff

Klicken Sie auf **Details**, um weitere Informationen zu einem bestimmten Ereignis anzuzeigen.

GFI MailEssentials-Ereignisse sind auch in der Windows-Ereignisanzeige unter **Anwendungs- und Dienstprotokolle** > GFI MailEssentials verfügbar.

4.1.5 POP2Exchange-Aktivitäten



Screenshot 29: POP2Exchange-Protokoll

Sie können in GFI MailEssentials die Aktivitäten von POP2Exchange in Echtzeit überwachen. Öffnen Sie **GFI MailEssentials > Dashboard**, und wählen Sie die Registerkarte **POP2Exchange** aus.

> **HINWEIS**
>
> Weitere Informationen finden Sie unter „POP2Exchange - E-Mails vom POP3-Server herunterladen“ (Seite 262).

4.2 Berichte

GFI MailEssentials ermöglicht das Erstellen von Berichten basierend auf Daten, die in einer Datenbank protokolliert sind.

Zum Öffnen der Berichterstellung wählen Sie **GFI MailEssentials > Berichterstellung** aus.

» **Aktivieren der Berichterstellung** - Weitere Informationen finden Sie unter „Aktivieren/Deaktivieren der Berichterstellung“ (Seite 61).

» **Konfigurieren der Berichtsdatenbank** - Weitere Informationen finden Sie unter „Konfigurieren der Berichtsdatenbank“ (Seite 68).

» **Erstellen eines Berichts** - Weitere Informationen finden Sie unter „Erstellen eines Berichts“ (Seite 62).

» **Erstellen Sie benutzerdefinierte Berichte**: Weitere Informationen finden Sie unter „Benutzerdefinierte Berichte“ (Seite 65).

» **Durchsuchen der Berichtsdatenbank** - Weitere Informationen finden Sie unter „Durchsuchen der Berichtsdatenbank“ (Seite 66).

4.2.1 Aktivieren/Deaktivieren der Berichterstellung

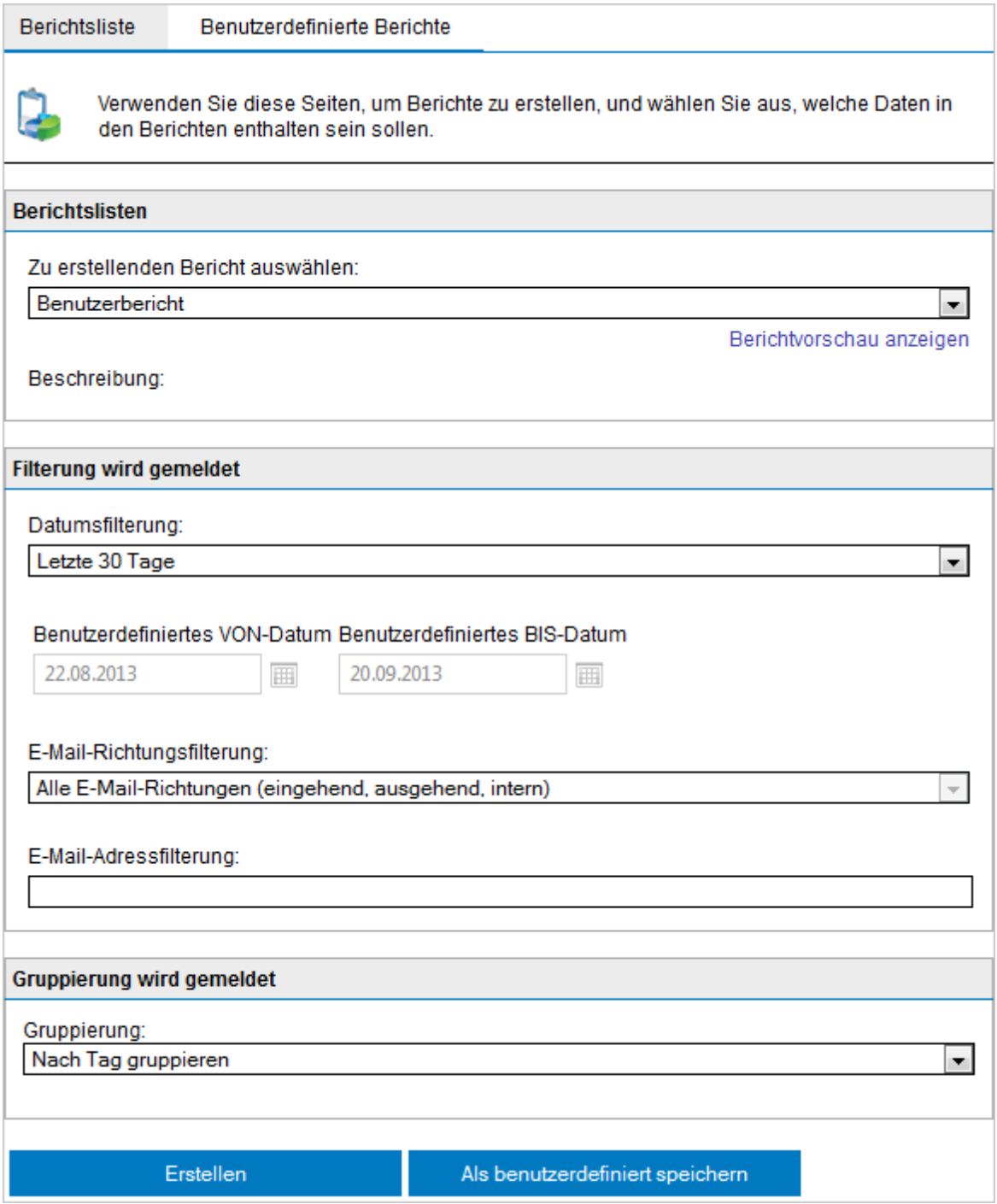
Die Berichterstellung ist standardmäßig aktiviert, und die E-Mail-Aktivitätsdaten werden in einer Microsoft® Access-Datenbank an folgendem Speicherort protokolliert:

<GFI MailEssentials Installationspfad>\GFI\MailEssentials\data\reports.mdb.

Navigieren Sie zum Knoten **Berichterstellung > Einstellungen**, und aktivieren oder deaktivieren Sie nach Bedarf die Option **Berichterstellung aktivieren.**

4.2.2 Erstellen eines Berichts

1. Navigieren Sie in GFI MailEssentials Configuration zu **GFI MailEssentials > Berichterstellung > Berichte.**

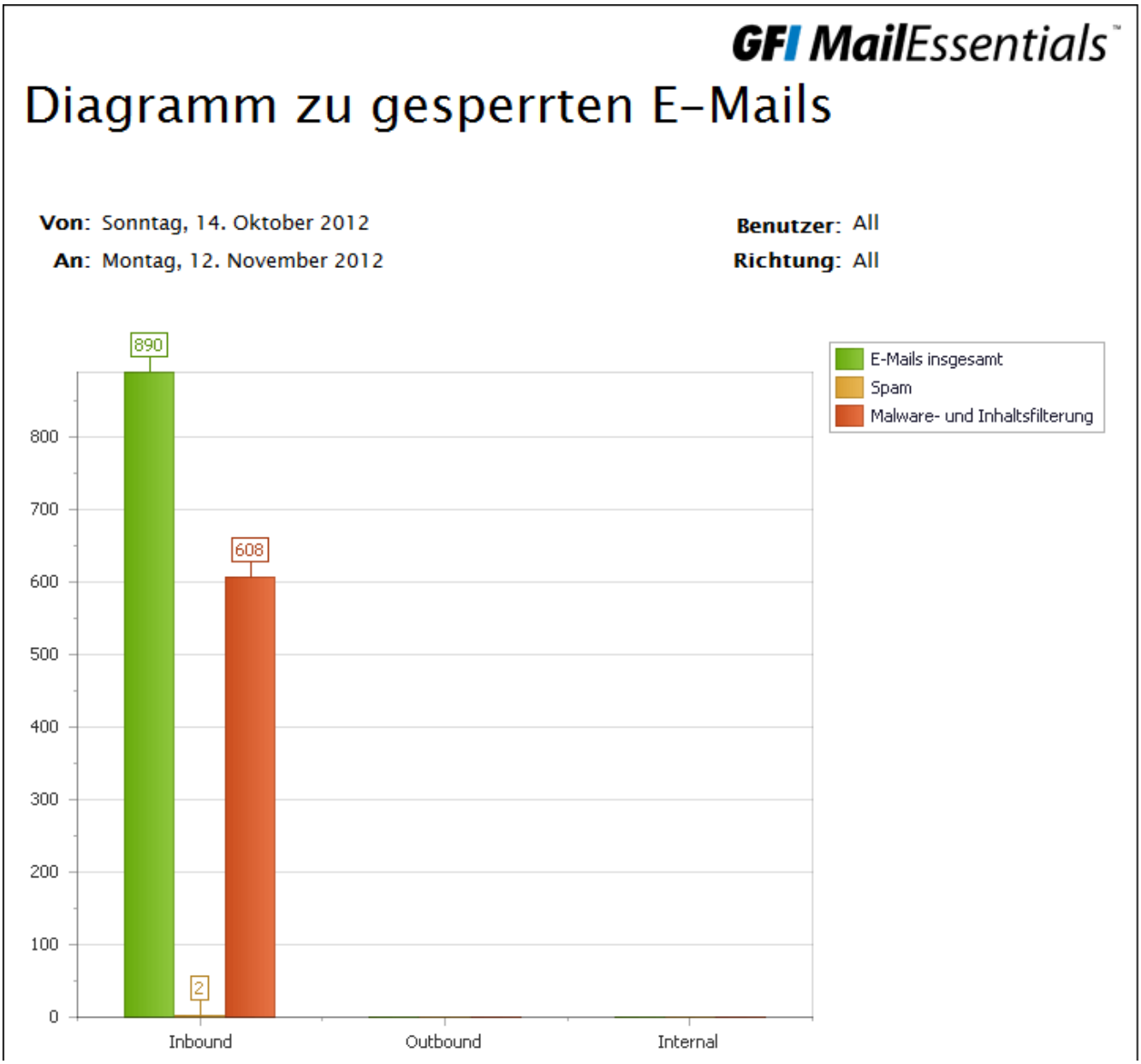


Screenshot 30: Erstellen eines Berichts

2. Konfigurieren Sie in der Registerkarte **Berichtliste** die folgenden Berichtsoptionen:

Option	Beschreibung
Berichtstyp	Wählen Sie den Berichtstyp aus, der erstellt werden soll: » **Blockierte E-Mails**: Zeigt an, wie viele der insgesamt verarbeiteten E-Mails von Anti-Spam- und Anti-Malware-Filtern in den verschiedenen Richtungen (eingehend, ausgehend und intern) blockiert wurden. » **Diagramm zu blockierten E-Mails**: Stellt grafisch dar, wie viele der insgesamt verarbeiteten E-Mails von Anti-Spam- und Anti-Malware-Filtern in den verschiedenen Richtungen (eingehend, ausgehend und intern) blockiert wurden. » **Diagramm zur E-Mail-Richtung** – Stellt grafisch dar, wie viele E-Mails in jeder Richtung (eingehend, ausgehend und intern) insgesamt verarbeitet wurden. » **E-Mail-Richtung**: Zeigt an, wie viele E-Mails in jeder Richtung (eingehend, ausgehend und intern) insgesamt verarbeitet wurden. » **Benutzerbericht**: Zeigt die Anzahl der blockierten und zugelassenen E-Mails für jede E-Mail-Adresse an. » **Spam-Filter**: Zeigt die Gesamtanzahl der von jedem Anti-Spam-Filter blockierten E-Mails. » **Spam-Filter-Diagramm**: Stellt die Gesamtanzahl der von jedem Anti-Spam-Filter blockierten E-Mails grafisch dar. Klicken Sie auf **Berichtvorschau anzeigen**, um eine Vorschau des Berichts anzuzeigen.
Datumsfilterung	Wählen Sie den Datumsbereich für den Bericht aus. Wenn Sie **Benutzerdefinierter Datumsbereich** auswählen, geben Sie mit den Kalendersteuerelementen **Benutzerdefiniertes VON-Datum** und **Benutzerdefiniertes BIS-Datum** den Zeitraum an, für den Daten angezeigt werden sollen.
E-Mail-Richtungsfilterung	Wählen Sie eine bestimmte E-Mail-Richtung aus, für die Daten angezeigt werden sollen, oder wählen Sie **Alle E-Mail-Richtungen (eingehend, ausgehende, intern)** aus, um die Daten für alle Richtungen anzuzeigen.
E-Mail-Adressfilterung	Geben Sie eine E-Mail-Adresse ein, um nur für diese Adresse Berichtsinformationen anzuzeigen.
Berichtsgruppierung	Geben Sie an, wie die Daten gruppiert werden sollen. Folgende Optionen sind verfügbar: » **Nach Tag gruppieren** » **Nach Woche gruppieren** » **Nach Monat gruppieren** » **Nach Jahr gruppieren**

3. Klicken Sie auf **Erstellen**, um den Bericht zu erstellen und anzuzeigen, oder klicken Sie auf **Als benutzerdefiniert speichern**, um die Berichteinstellungen zur späteren Wiederverwendung zu speichern.



Screenshot 31: Diagrammbericht zu blockierten E-Mails

Berichtsfunktionen

Mithilfe der Symbolleiste über dem Bericht können Sie folgende Funktionen nutzen:

Funktion	Symbol	Beschreibung
Drucken		Klicken Sie auf das Symbol, um den Bericht zu drucken.
Aktuelle Seite drucken		Klicken Sie auf das Symbol, um die angezeigte Seite zu drucken.
Navigieren		Verwenden Sie diese Symbolleiste, um die gewünschten Berichtsseiten anzuzeigen.
Speichern		Wählen Sie das Format aus, in dem der Bericht gespeichert werden soll, und klicken Sie auf **Speichern**. Geben Sie den gewünschten Speicherort für den Bericht an.

4.2.3 Benutzerdefinierte Berichte

In benutzerdefinierten Berichten, die Sie nach Zeitplan erstellen können, lassen sich konkrete Berichtparameter speichern (beispielsweise ein Berichttyp für einen konkreten Zeit-/Datumsbereich). Mit dieser Funktionen können Sie die Berichterstellung automatisieren.

Konfigurieren benutzerdefinierter Berichte

1. Navigieren Sie in GFI MailEssentials Configuration zu **GFI MailEssentials > Berichterstellung > Berichte**.

2. Wählen Sie die Registerkarte **Benutzerdefiniert Berichte** und klicken Sie auf **Neu**.

3. Konfigurieren Sie die folgenden Optionen:

Option	Beschreibung
Berichtstyp	Wählen Sie den Berichtstyp aus, der erstellt werden soll: » **Blockierte E-Mails**: Zeigt an, wie viele der insgesamt verarbeiteten E-Mails von Anti-Spam- und Anti-Malware-Filtern in den verschiedenen Richtungen (eingehend, ausgehend und intern) blockiert wurden. » **Diagramm zu blockierten E-Mails**: Stellt grafisch dar, wie viele der insgesamt verarbeiteten E-Mails von Anti-Spam- und Anti-Malware-Filtern in den verschiedenen Richtungen (eingehend, ausgehend und intern) blockiert wurden. » **Diagramm zur E-Mail-Richtung** – Stellt grafisch dar, wie viele E-Mails in jeder Richtung (eingehend, ausgehend und intern) insgesamt verarbeitet wurden. » **E-Mail-Richtung**: Zeigt an, wie viele E-Mails in jeder Richtung (eingehend, ausgehend und intern) insgesamt verarbeitet wurden. » **Benutzerbericht**: Zeigt die Anzahl der blockierten und zugelassenen E-Mails für jede E-Mail-Adresse an. » **Spam-Filter**: Zeigt die Gesamtanzahl der von jedem Anti-Spam-Filter blockierten E-Mails. » **Spam-Filter-Diagramm**: Stellt die Gesamtanzahl der von jedem Anti-Spam-Filter blockierten E-Mails grafisch dar. Klicken Sie auf **Berichtvorschau anzeigen**, um eine Vorschau des Berichts anzuzeigen.
Datumsfilterung	Wählen Sie den Datumsbereich für den Bericht aus. Wenn Sie **Benutzerdefinierter Datumsbereich** auswählen, geben Sie mit den Kalendersteuerelementen **Benutzerdefiniertes VON-Datum** und **Benutzerdefiniertes BIS-Datum** den Zeitraum an, für den Daten angezeigt werden sollen.
E-Mail-Richtungsfilterung	Wählen Sie eine bestimmte E-Mail-Richtung aus, für die Daten angezeigt werden sollen, oder wählen Sie **Alle E-Mail-Richtungen (eingehend, ausgehende, intern)** aus, um die Daten für alle Richtungen anzuzeigen.
E-Mail-Adressfilterung	Geben Sie eine E-Mail-Adresse ein, um nur für diese Adresse Berichtsinformationen anzuzeigen.
Berichtsgruppierung	Geben Sie an, wie die Daten gruppiert werden sollen. Folgende Optionen sind verfügbar: » **Nach Tag gruppieren** » **Nach Woche gruppieren** » **Nach Monat gruppieren** » **Nach Jahr gruppieren**

4. Optional können Sie auch das Kontrollkästchen **Senden alle/jeden** aktivieren und eine Kombination aus Datum und Uhrzeit für die Berichterstellung festlegen. Klicken Sie auf **Regel hinzufügen**, um die Zeit für die Berichterstellung zu speichern.

HINWEIS:

Zum Löschen einer Regel wählen Sie eine vorhandene Berichterstellungszeit aus, und klicken Sie auf **Löschen**.

5. Legen Sie fest, ob der Bericht per E-Mail gesdendet oder auf dem Datenträger gespeichert wird. Um den Bericht per E-Mail zu senden, wählen Sie **Per E-Mail senden** und geben Sie die E-Mail-Adresse des Empfängers an. Um den Bericht auf dem Datenträger zu specihern, klicken Sie auf **Auf Festplatte speichern**, und geben Sie einen Speicherort sowie das Format für die zu speichernde Datei an.

6. Klicken Sie auf **Speichern**, um den neu angelegten Bericht zu speichern.

4.2.4 Erstellen benutzerdefinierter Berichte

Einen benutzerdefinierten Bericht erstellen:

1. Navigieren Sie in GFI MailEssentials Configuration zu **GFI MailEssentials > Berichterstellung > Berichte**.

2. Wählen Sie in der Registerkarte **Benutzerdefinierte Berichte** einen Bericht aus, den Sie erstellen möchten.

3. Klicken Sie auf **Erstellen**.

4.2.5 Löschen benutzerdefinierter Berichte

Einen benutzerdefinierten Bericht löschen:

1. Navigieren Sie in GFI MailEssentials Configuration zu **GFI MailEssentials > Berichterstellung > Berichte**.

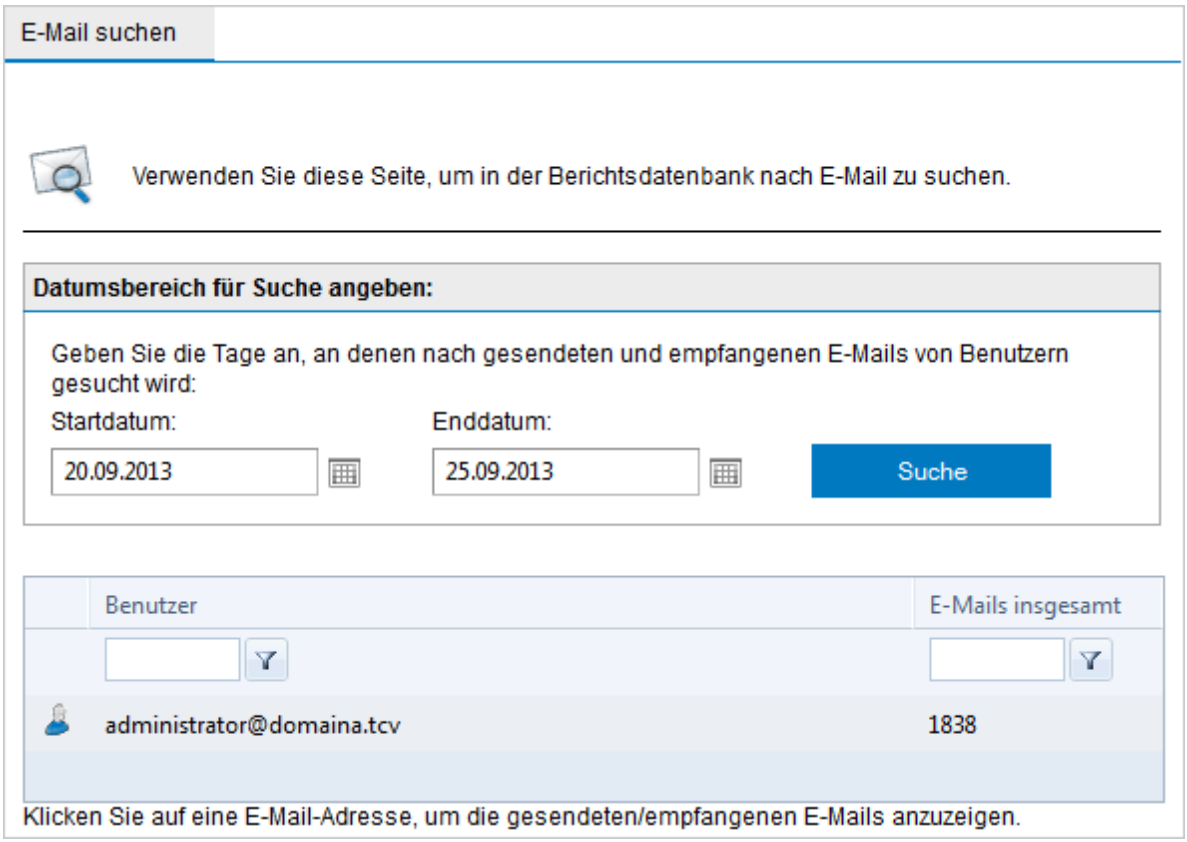
2. Wählen Sie in der Registerkarte **Benutzerdefinierte Berichte** einen Bericht aus, den Sie löschen möchten.

3. Klicken Sie auf **Löschen**.

4.2.6 Durchsuchen der Berichtsdatenbank

GFI MailEssentials speichert die Eigenschaften aller verarbeiteten E-Mails in der Berichtsdatenbank. GFI MailEssentials ermöglicht das Durchsuchen der Berichtsdatenbank nach bestimmten verarbeiteten E-Mails. So durchsuchen Sie die Berichtsdatenbank:

1. Navigieren Sie in GFI MailEssentials Configuration zu **GFI MailEssentials > Berichterstellung > Suche**.

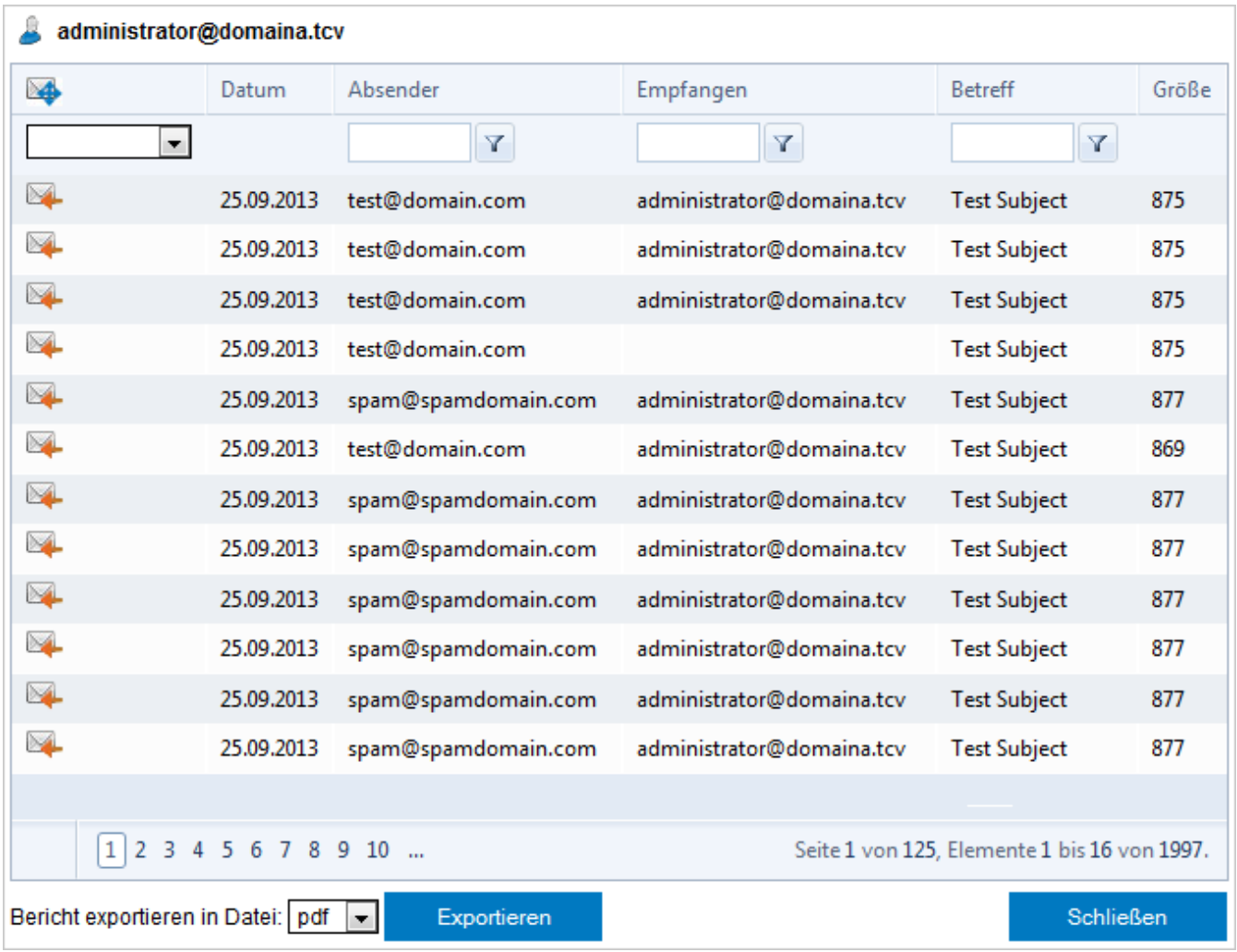


Screenshot 32: Durchsuchen der Berichtsdatenbank

2. Geben Sie Ihre Suchkriterien an:

Suchkriterien	Beschreibung
Startdatum und **Enddatum**	Wählen Sie einen Datumsbereich aus, um E-Mails aus diesem Zeitraum zu filtern. Klicken Sie auf **Suchen**.
Benutzer	Filtert die E-Mail-Adressen. Geben Sie eine Zahl ein, und klicken Sie auf , um die Bedingungen festzulegen.
E-Mails insgesamt	Filtert Benutzer nach der Anzahl der verarbeiteten E-Mails. Geben Sie eine Zahl ein, und klicken Sie auf , um die Bedingungen festzulegen.

3. Die Liste der übereinstimmenden Benutzer wird angezeigt. Klicken Sie auf eine E-Mail-Adresse, um einen detaillierten Bericht der für diese Adresse verarbeiteten E-Mails anzuzeigen.


administrator@domaina.tcv
Datum
Absender
Empfangen
Betreff
Größe
25.09.2013 test@domain.com administrator@domaina.tcv Test Subject 875
25.09.2013 test@domain.com administrator@domaina.tcv Test Subject 875
25.09.2013 test@domain.com administrator@domaina.tcv Test Subject 875
25.09.2013 test@domain.com Test Subject 875
25.09.2013 spam@spamdomain.com administrator@domaina.tcv Test Subject 877
25.09.2013 test@domain.com administrator@domaina.tcv Test Subject 869
25.09.2013 spam@spamdomain.com administrator@domaina.tcv Test Subject 877
25.09.2013 spam@spamdomain.com administrator@domaina.tcv Test Subject 877
25.09.2013 spam@spamdomain.com administrator@domaina.tcv Test Subject 877
25.09.2013 spam@spamdomain.com administrator@domaina.tcv Test Subject 877
25.09.2013 spam@spamdomain.com administrator@domaina.tcv Test Subject 877
25.09.2013 spam@spamdomain.com administrator@domaina.tcv Test Subject 877
1 2 3 4 5 6 7 8 9 10 ...
Seite 1 von 125, Elemente 1 bis 16 von 1997.
Bericht exportieren in Datei: pdf
Exportieren
Schließen

Screenshot 33: Suchergebnisse aus der Berichtsdatenbank

4. Im Bericht können Sie die Daten optional nach E-Mail-Richtung, Absender, Empfänger oder Betreff filtern.

5. Um den Bericht in einem anderen Format zu exportieren, wählen Sie das Format aus, und klicken Sie auf **Exportieren**.

4.2.7 Konfigurieren der Berichtsdatenbank

GFI MailEssentials verwendet standardmäßig eine Microsoft® Access-Datenbank mit der Bezeichnung **reports.mdb**, die sich an folgendem Speicherort befindet:

```
<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\data\
```

Sie können auch eine Microsoft® SQL Server-Datenbank für Berichte verwenden.

» Konfigurieren eines Microsoft® Access-Datenbank-Backends

» Konfigurieren eines Microsoft® SQL Server-Datenbank-Backends

» Konfigurieren der automatischen Datenbankbereinigung

Konfigurieren eines Microsoft® Access-Datenbank-Backends

Berichterstellung
Automatische Bereinigung
Konfigurieren Sie die Berichtsdatenbank.
Verwenden Sie diesen Knoten, um die Berichterstellung von GFI MailEssentials zu aktivieren und zu verwenden. Diese Option ermöglicht es mit den von GFI MailEssentials gesammelten Daten verschiedene Berichte zu erstellen.
Berichterstellung aktivieren
Aktuelle Datenbankeinstellungen
Aktueller Typ:
Microsoft Access
Aktueller Speicherort:
C:\Program Files (x86)\GFI\MailEssentials\data\reports.mdb
Neue Datenbankeinstellungen
Datenbanktyp
MS Access
SQL Server
Microsoft Access-Berichterstellung
Geben Sie nachfolgend einen gültigen Pfad zu einer vorhandenen Datenbank ein, oder geben Sie einen neuen Speicherort/Dateinamen an, um automatisch eine neue Datenbank zu erstellen.
Datei:
C:\Program Files (x86)\GFI\MailEssentials\data\reports.mdb

Screenshot 34: Konfigurieren eines Microsoft® Access-Datenbank-Backends

1. Wählen Sie **Berichterstellung > Einstellungen** aus.

2. Wählen Sie **MS Access** aus.

3. Geben Sie den vollständigen Pfad einschließlich des Dateinamens (und der Erweiterung .mdb) der Datenbankdatei ein. Wenn Sie nur einen Dateinamen angeben, wird die Datenbankdatei unter folgendem Standardpfad erstellt:

`<GFI MailEssentials Installationspfad>\GFI\MailEssentials\data\`

4. Klicken Sie auf **Übernehmen**.

Konfigurieren eines Microsoft® SQL Server-Datenbank-Backends

1. Erstellen Sie in Microsoft® SQL Server eine neue Datenbank.

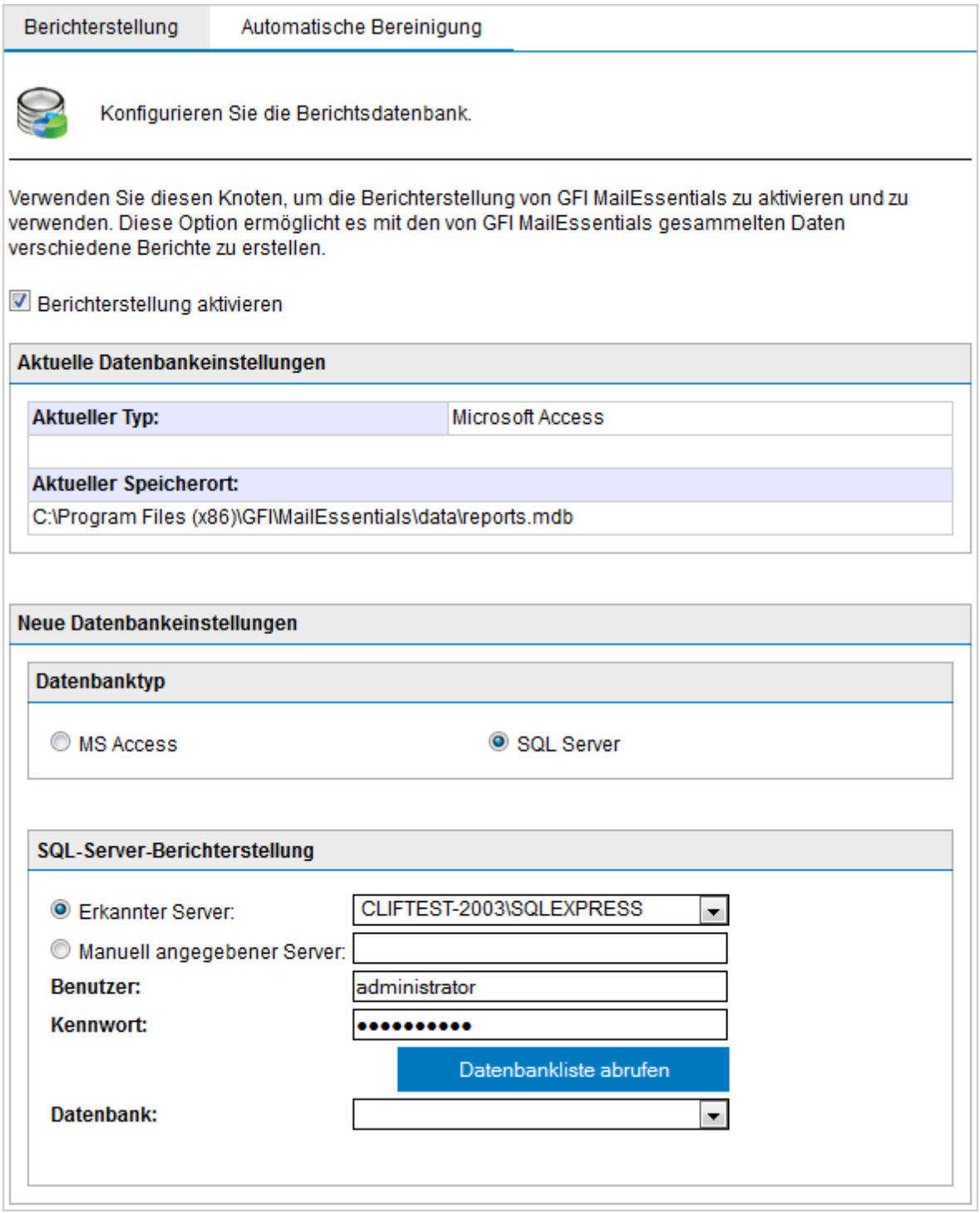
HINWEIS

Es wird empfohlen, in Microsoft® SQL Server einen dedizierten Benutzer/Anmeldenamen für GFI MailEssentials zu erstellen und diesem die Rolle des Systemadministrators zuzuweisen.

HINWEIS

Weitere Informationen zum Erstellen einer neuen Datenbank in Microsoft® SQL Server finden Sie unter http://go.gfi.com/?pageid=ME_newSQLdb.

2. Wählen Sie **Berichterstellung > Einstellungen** aus.



Screenshot 35: Konfigurieren eines SQL Server-Datenbank-Backends

3. Wählen Sie **SQL Server** aus.

4. Wählen Sie **Erkannter Server** und anschließend den automatisch erkannten SQL-Server in der Liste aus. Wird der Server nicht erkannt, wählen Sie **Manuell angegebener Server** aus, und geben Sie die IP-Adresse oder den Servernamen des Microsoft® SQL Server ein.

5. Geben Sie die Anmeldeinformationen mit Lese- und Schreibberechtigung für die Datenbank ein.

6. Klicken Sie auf **Datenbankliste abrufen**, um die Liste der Datenbanken vom Server abzurufen.

7. Wählen Sie aus der Liste **Datenbank** die Datenbank aus, die für die GFI MailEssentials-Berichterstellung erstellt wurde.

8. Klicken Sie auf **Übernehmen**.

Konfigurieren der automatischen Datenbankbereinigung

Sie können GFI MailEssentials so konfigurieren, dass Einträge in der Datenbank, die ein bestimmtes Alter erreicht haben, automatisch gelöscht (bereinigt) werden. So aktivieren Sie die automatische Bereinigung:

1. Wählen Sie **Berichterstellung > Einstellungen** und anschließend die Registerkarte **Automatische Bereinigung** aus.

2. Wählen Sie **Automatische Bereinigung aktivieren** aus, und geben Sie an, für wie viele Monate Elemente in der Datenbank gespeichert werden sollen.

> **HINWEIS**
>
> Die automatische Bereinigung wird nur auf die aktuelle Datenbank angewendet, die auf der Registerkarte Berichterstellung konfiguriert wurde.

3. Klicken Sie auf **Übernehmen**.

4.2.8 MailInsights®-Bericht

GFI MailInsights® ist eine Reporting-Instanz, welche die Daten der Berichtsdatenbank nutzt, um Informationen bezüglich der E-Mail-Nutzung und Tendenzen bereitzustellen.

GFI MailEssentials stellt den Kommunikationsflussbericht bereit, der eine grafische Darstellung der zwischen ausgewählten Benutzern/Gruppen und deren Kontakten ausgetauschten E-Mails enthält. Weitere MailInsights®-Berichte können mithilfe von GFI MailArchiver erstellt werden.

Kommunikationsflussbericht

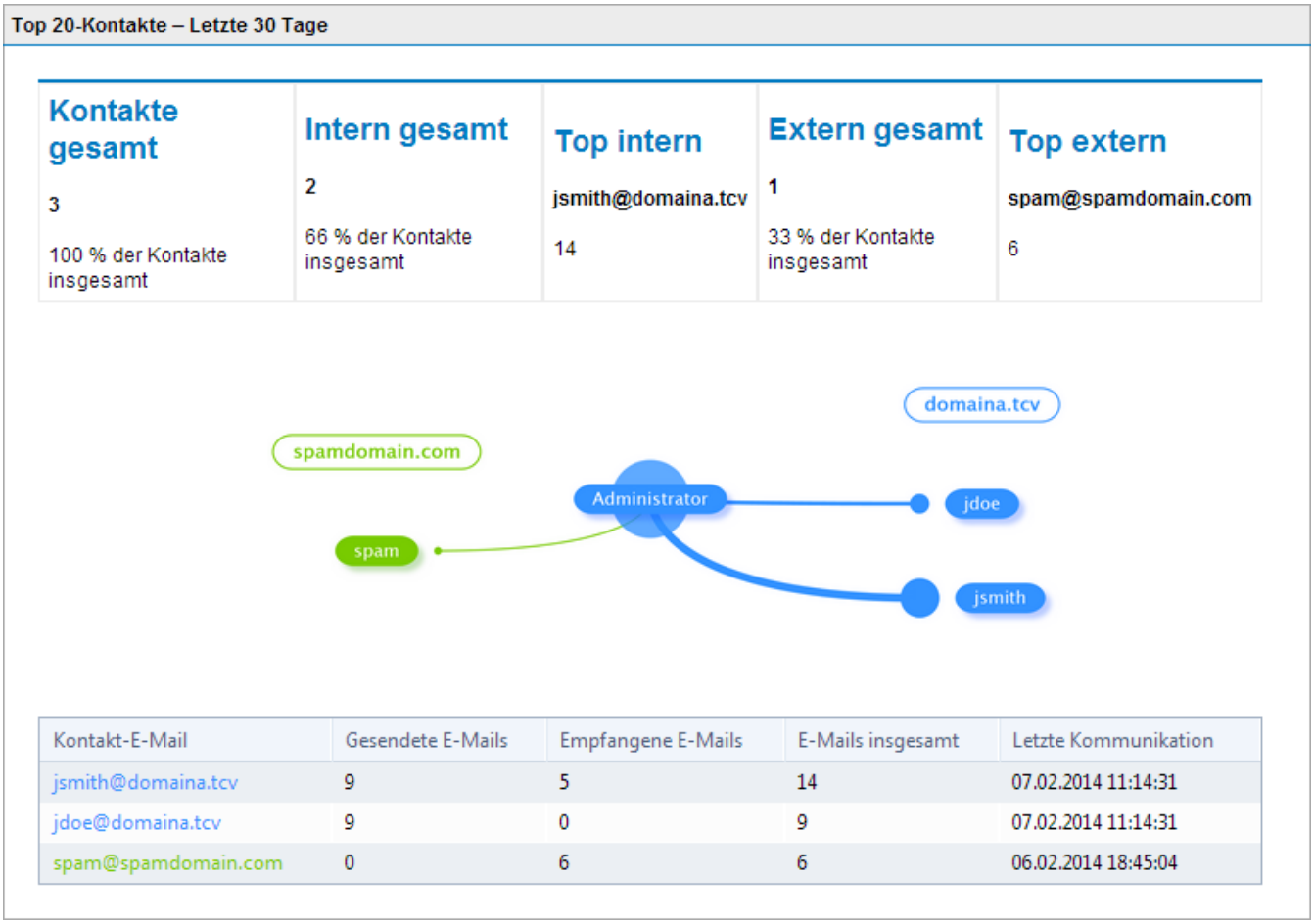
Der Kommunikationsflussbericht zeigt die Top 20-Kontakte, mit denen ein Benutzer in den letzten 30 Tagen kommuniziert hat.

1. Wählen Sie **Berichterstellung > MailInsights** und anschließend die Registerkarte **Kommunikationsfluss** aus.

2. Administratoren können den Bericht für jeden E-Mail-Benutzer erstellen. Klicken Sie auf **Suchen**, um einen E-Mail-Benutzer auszuwählen. Klicken Sie anschließend auf **Erstellen**, um die Berichterstellung zu starten.

Der generierte Bericht zeigt die Daten für den ausgewählten Benutzer wie folgt an:

Gesamt	Der obere Bereich des Berichts enthält die Gesamtstatistik des Kommunikationsflusses der letzten 30 Tage. » **Kontakte gesamt** - Die Gesamtanzahl der E-Mail-Adressen, mit denen der Benutzer Kontakt hatte. » **Intern gesamt** - Die Gesamtanzahl der internen Benutzer, mit denen der Benutzer kommuniziert hat. » **Top intern** - Die interne E-Mail-Adresse, mit der der ausgewählte Benutzer am meisten kommuniziert hat. » **Extern gesamt** - Die Gesamtanzahl der externen Benutzer, mit denen der Benutzer kommuniziert hat. » **Top extern** - Die externe E-Mail-Adresse, mit der der ausgewählte Benutzer am meisten kommuniziert hat.
Diagramm	Der ausgewählte Benutzer wird als eine einzelne Einheit in der Mitte des Diagramms angezeigt. Kontakte werden nach Domänen getrennt. Jedes Domänen-Cluster wird in einer anderen Farbe dargestellt. Die Randbreite zwischen den Knoten zeigt die Intensität der E-Mail-Beziehung zwischen verschiedenen Entitäten an.
Top 20-Kontakte	Die Top 20-Kontakte, mit denen der ausgewählte Benutzer am meisten kommuniziert hat. Unterschiedliche Farben zeigen die unterschiedlichen Domänen der Kontakte an. Die Tabelle enthält die Gesamtanzahl der gesendeten und empfangenen E-Mails dieses Kontakts zusammen mit dem Datum und der Uhrzeit der letzten E-Mail-Kommunikation.



5 E-Mail-Sicherheit

Die Sicherheitsfilter von GFI MailEssentials bieten Schutz vor mit Viren infizierten und anderen schädlichen E-Mails.

Themen in diesem Kapitel:

5.1 Virenscan-Engines **73**

5.2 Informationsspeicherschutz **96**

5.3 Scanner für Trojaner und ausführbare Dateien **99**

5.4 E-Mail-Exploit-Engine **103**

5.5 HTML-Bereinigung **107**

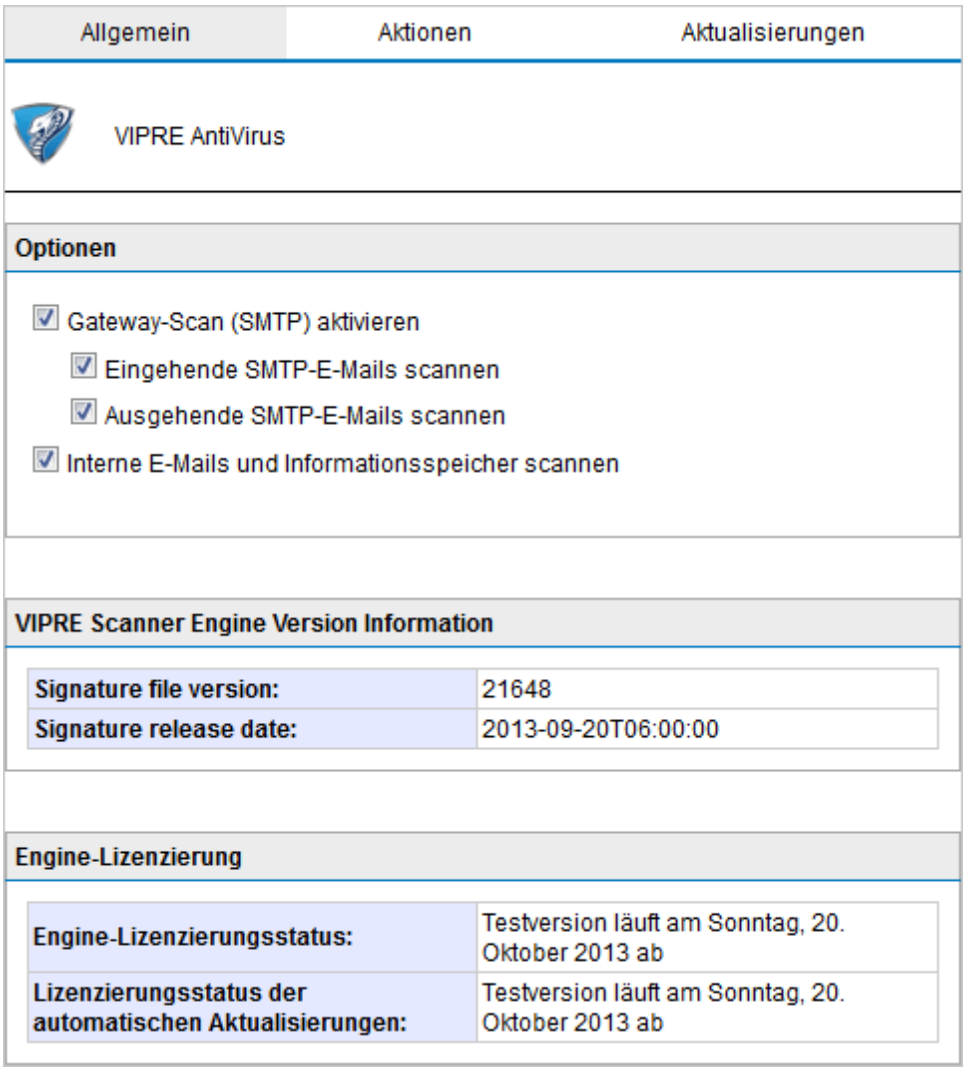
5.1 Virenscan-Engines

GFI MailEssentials verwendet mehrere Anti-Virus-Engines, um eingehende, ausgehende und interne E-Mails auf Viren zu scannen. GFI MailEssentials beinhaltet die Virenscan-Engines Vipre und BitDefender. Sie können auch eine Lizenz für Norman, Kaspersky und McAfee erwerben.

In diesem Kapitel wird beschrieben, wie Sie Virenscan-Engines, Aktualisierungen, Aktionen und die Scanreihenfolge konfigurieren.

5.1.1 Vipre

1. Wählen Sie **E-Mail-Sicherheit > Virenscan-Engines > Vipre** aus.



Screenshot 36: Konfiguration von Vipre

2. Aktivieren Sie das Kontrollkästchen **Gateway-Scan (SMTP) aktivieren**, um E-Mails mit dieser Virenscan-Engine zu prüfen.

3. Wählen Sie aus, ob eingehende und/oder ausgehende E-Mails mit dieser Virenscan-Engine gescannt werden sollen.

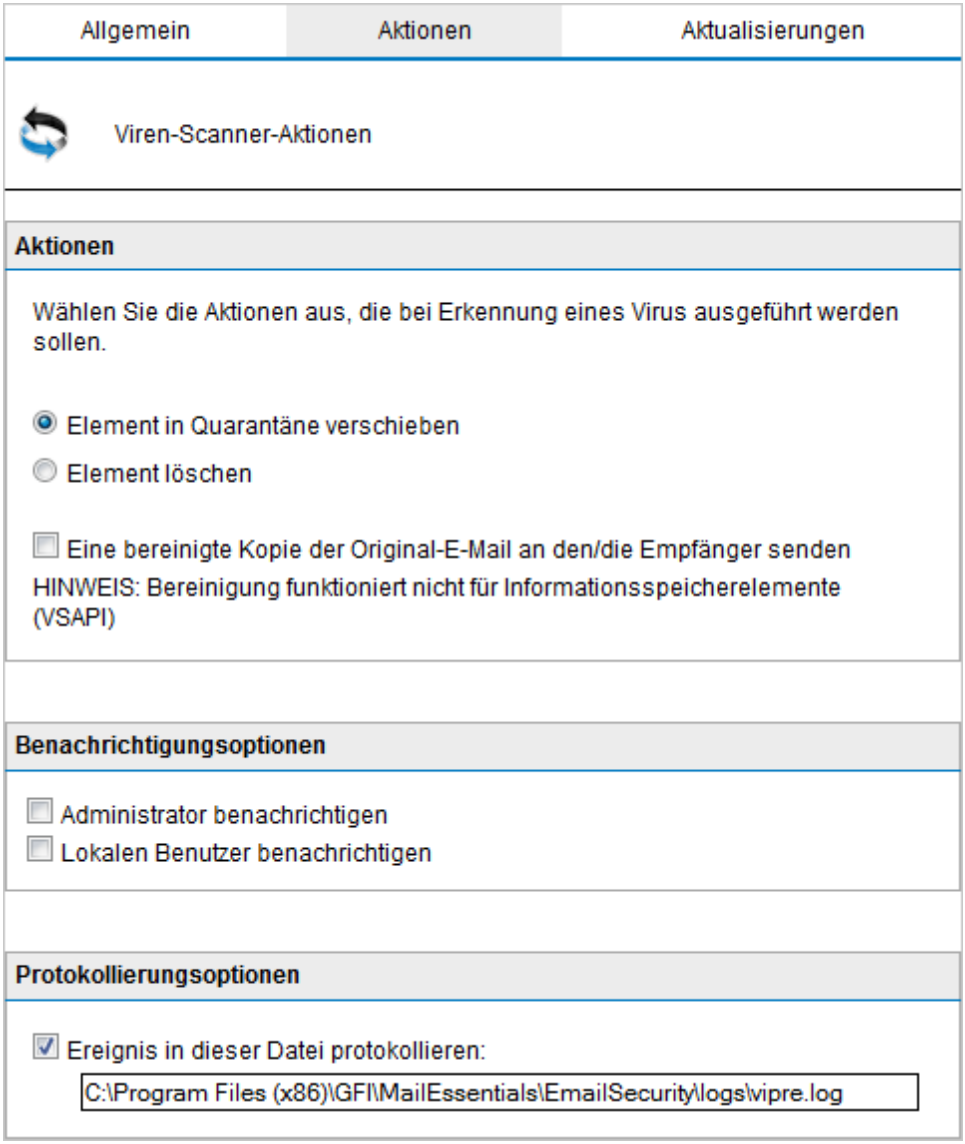
Option	Beschreibung
Eingehende SMTP-E-Mails scannen	Wählen Sie diese Option aus, um eingehende E-Mails zu scannen.
Ausgehende SMTP-E-Mails scannen	Wählen Sie diese Option aus, um ausgehende E-Mails zu scannen.

4. Wenn Sie GFI MailEssentials auf einem Microsoft® Exchange-Rechner installiert haben, können Sie auch interne E-Mails und den Informationsspeicher scannen. Wählen Sie **Interne E-Mails und Informationsspeicherelemente scannen** aus.

> **HINWEIS**
>
> Um den Virenscan des Informationsspeichers zu verwenden, müssen Sie die Option im Knoten **Informationsspeicherschutz** aktivieren. Weitere Informationen finden Sie unter „Informationsspeicherschutz“ (Seite 96).

HINWEIS

Auf dieser Seite können Sie auch die Lizenz- und Versionsinformationen der Anti-Virus-Engine überprüfen.



Screenshot 37: Aktionen der Virenscan-Engine

5. Wählen Sie auf der Registerkarte **Aktionen** aus, was geschehen soll, wenn eine E-Mail blockiert wird:

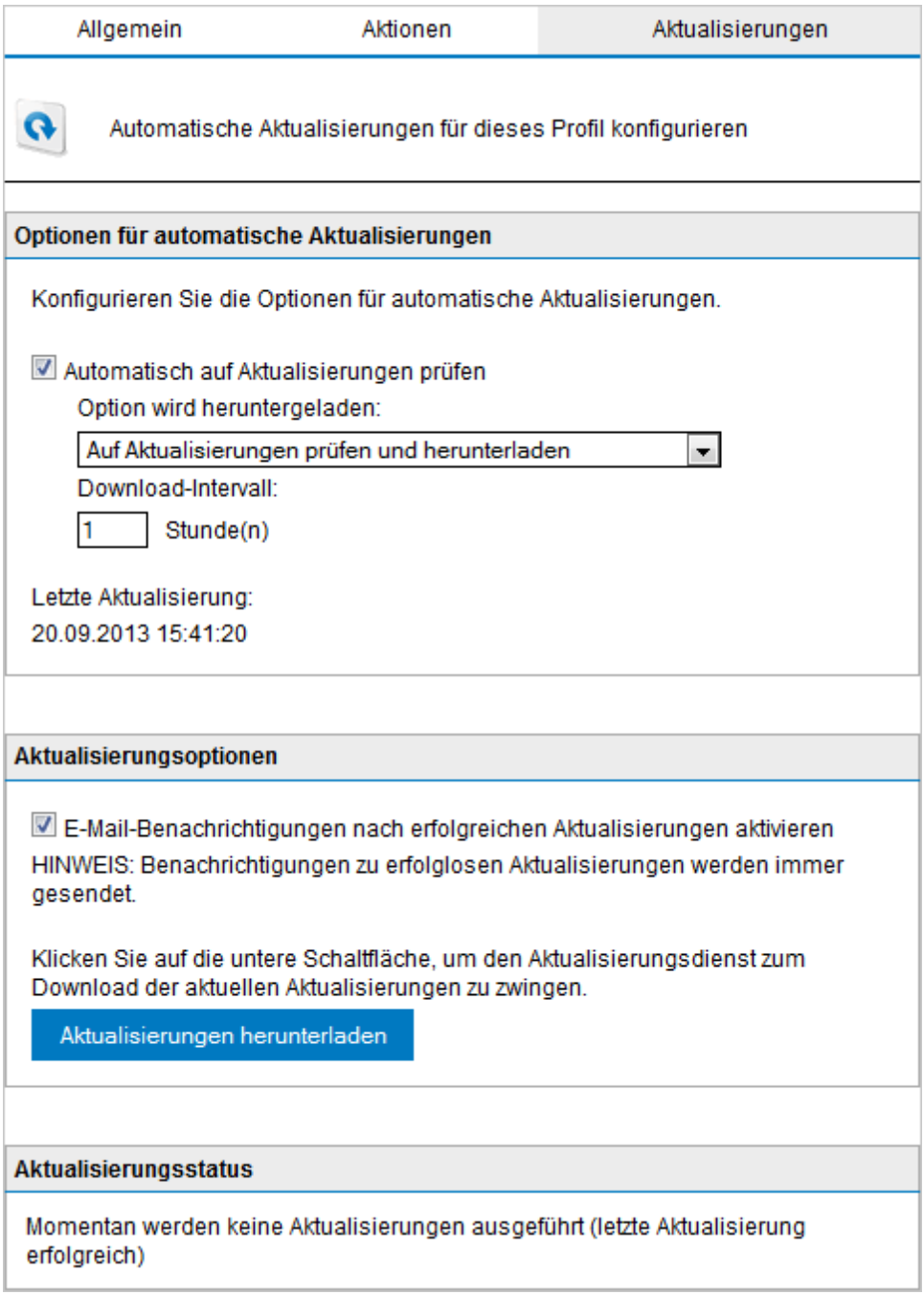
Aktion	Beschreibung
E-Mail in Quarantäne verschieben	Speichert alle infizierten E-Mails, die von der ausgewählten Virenscan-Engine erkannt werden, im Quarantänespeicher. Danach können Sie alle E-Mails in der Quarantäne überprüfen (zulassen/löschen). Weitere Informationen finden Sie unter „Quarantäne“ (Seite 208).
E-Mail löschen	Löscht infizierte E-Mails
Eine bereinigte Kopie der Original-E-Mail in die Empfänger senden	Wählen Sie aus, ob eine bereinigte Kopie der blockierten E-Mail an die Empfänger gesendet werden soll.

6. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

7. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

`<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log`



Screenshot 38: Aktualisierungen für Virenscan-Engines

8. Wählen Sie auf der Registerkarte **Aktualisierungen** die Option **Automatisch auf Aktualisierungen prüfen** aus, um die automatische Aktualisierung der Anti-Virus-Dateien für die ausgewählte Engine zu aktivieren.

9. Wählen Sie in der Liste **Download-Option** eine der folgenden Optionen aus:

Option	Beschreibung
Nur auf Aktualisierungen prüfen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach Aktualisierungen suchen und den Administrator benachrichtigen soll, sobald Aktualisierungen für diese Engine verfügbar sind. Mit dieser Option werden die verfügbaren Aktualisierungen NICHT automatisch heruntergeladen.
Auf Aktualisierungen prüfen und herunterladen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach verfügbaren Aktualisierungen für diese Engine suchen und diese automatisch herunterladen soll.

10. Geben Sie in Form eines Stundenintervalls an, wie oft GFI MailEssentials nach Aktualisierungen für diese Engine suchen bzw. diese herunterladen soll.

11. Wählen Sie im Bereich **Aktualisierungsoptionen** die Option **E-Mail-Benachrichtigungen nach erfolgreichen Aktualisierungen aktivieren**, um eine Benachrichtigung an den Administrator zu senden, wenn die Engine erfolgreich aktualisiert wurde.

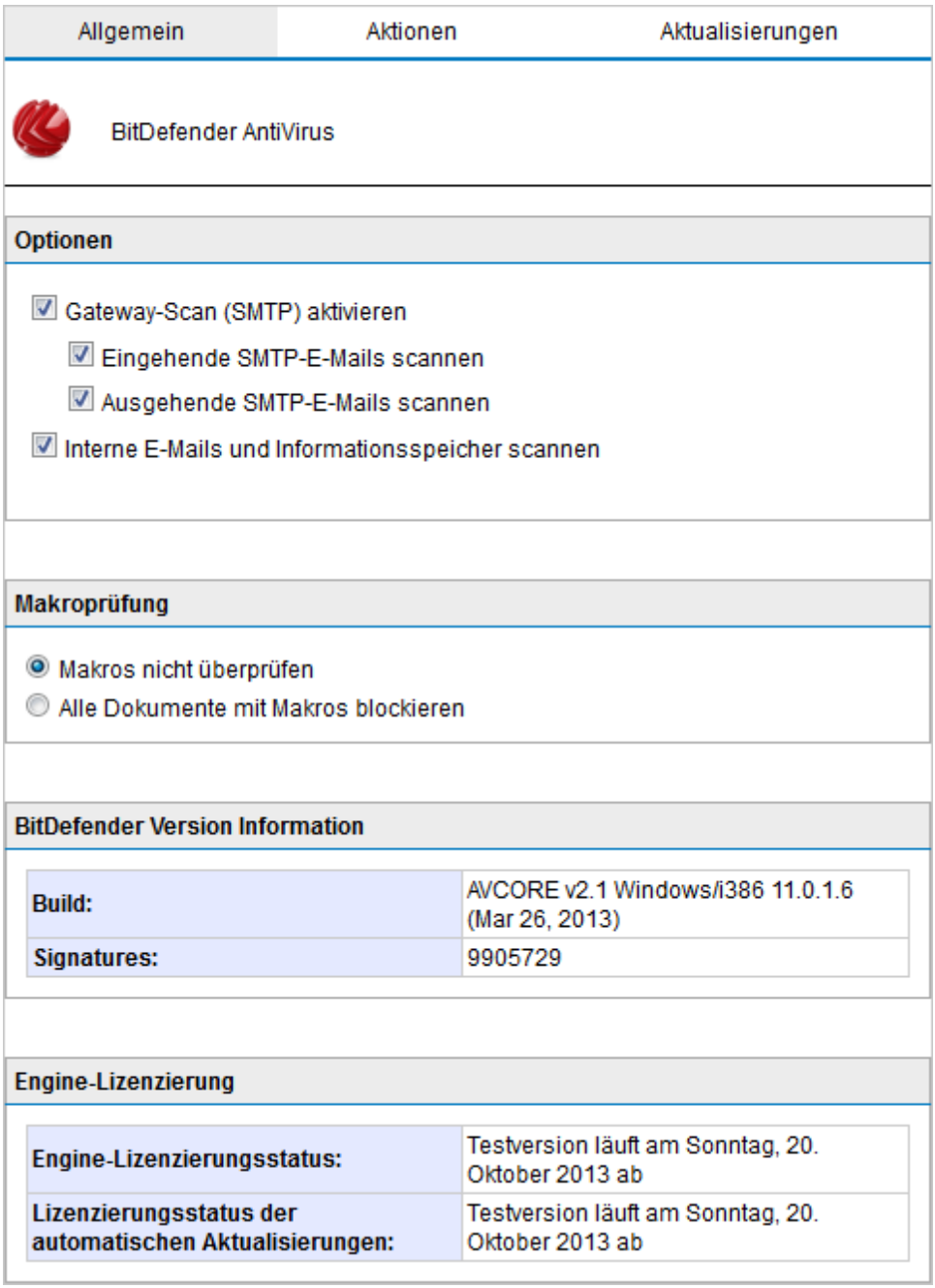
> **HINWEIS**
>
> Wenn Aktualisierungen fehlschlagen, wird immer eine E-Mail-Benachrichtigung gesendet.

12. Klicken Sie auf **Aktualisierungen herunterladen**, um sofort nach Aktualisierungen zu suchen und diese herunterzuladen.

13. Klicken Sie auf **Übernehmen**.

5.1.2 BitDefender

1. Wählen Sie **E-Mail-Sicherheit > Virenscan-Engines > BitDefender** aus.



Screenshot 39: Konfiguration von BitDefender

2. Aktivieren Sie das Kontrollkästchen **Gateway-Scan (SMTP) aktivieren**, um E-Mails mit dieser Virenscan-Engine zu prüfen.

3. Wählen Sie aus, ob eingehende und/oder ausgehende E-Mails mit dieser Virenscan-Engine gescannt werden sollen.

Option	Beschreibung
Eingehende SMTP-E-Mails scannen	Wählen Sie diese Option aus, um eingehende E-Mails zu scannen.
Ausgehende SMTP-E-Mails scannen	Wählen Sie diese Option aus, um ausgehende E-Mails zu scannen.

4. Wenn Sie GFI MailEssentials auf einem Microsoft® Exchange-Rechner installiert haben, können Sie auch interne E-Mails und den Informationsspeicher scannen. Wählen Sie **Interne E-Mails und Informationsspeicherelemente scannen** aus.

HINWEIS

Um den Virenscan des Informationsspeichers zu verwenden, müssen Sie die Option im Knoten **Informationsspeicherschutz** aktivieren. Weitere Informationen finden Sie unter „Informationsspeicherschutz“ (Seite 96).

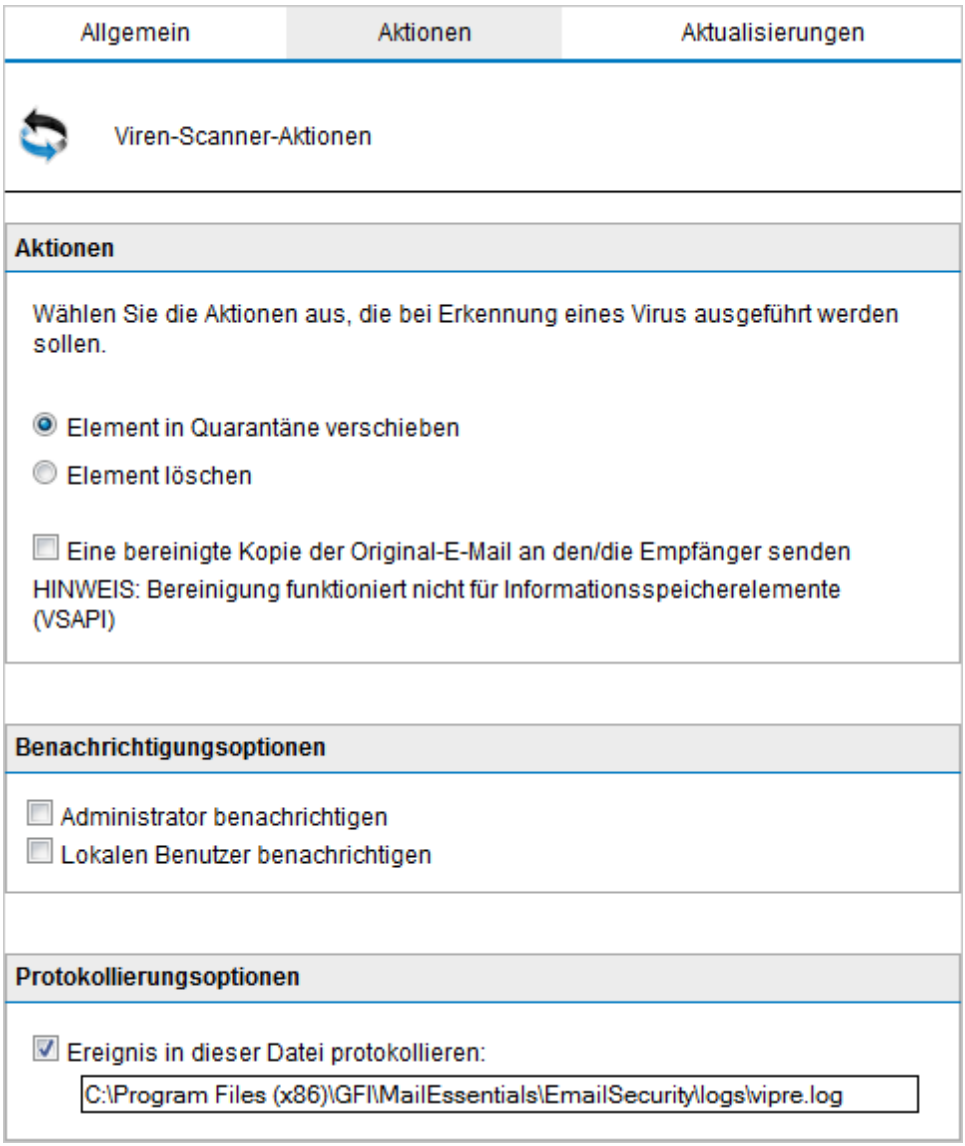
HINWEIS

Auf dieser Seite können Sie auch die Lizenz- und Versionsinformationen der Anti-Virus-Engine überprüfen.

5. Mit BitDefender können auch E-Mails mit Anhängen blockiert werden, die Makros enthalten. Sie aktivieren diese Funktion, indem Sie im Bereich **Makroprüfung** die Option **Alle Dokumente mit Makros blockieren** auswählen.

HINWEIS

Auch wenn die Makroprüfung deaktiviert ist, sucht GFI MailEssentials trotzdem nach Makroviren und blockiert sie.



Screenshot 40: Aktionen der Virenscan-Engine

6. Wählen Sie auf der Registerkarte **Aktionen** aus, was geschehen soll, wenn eine E-Mail blockiert wird:

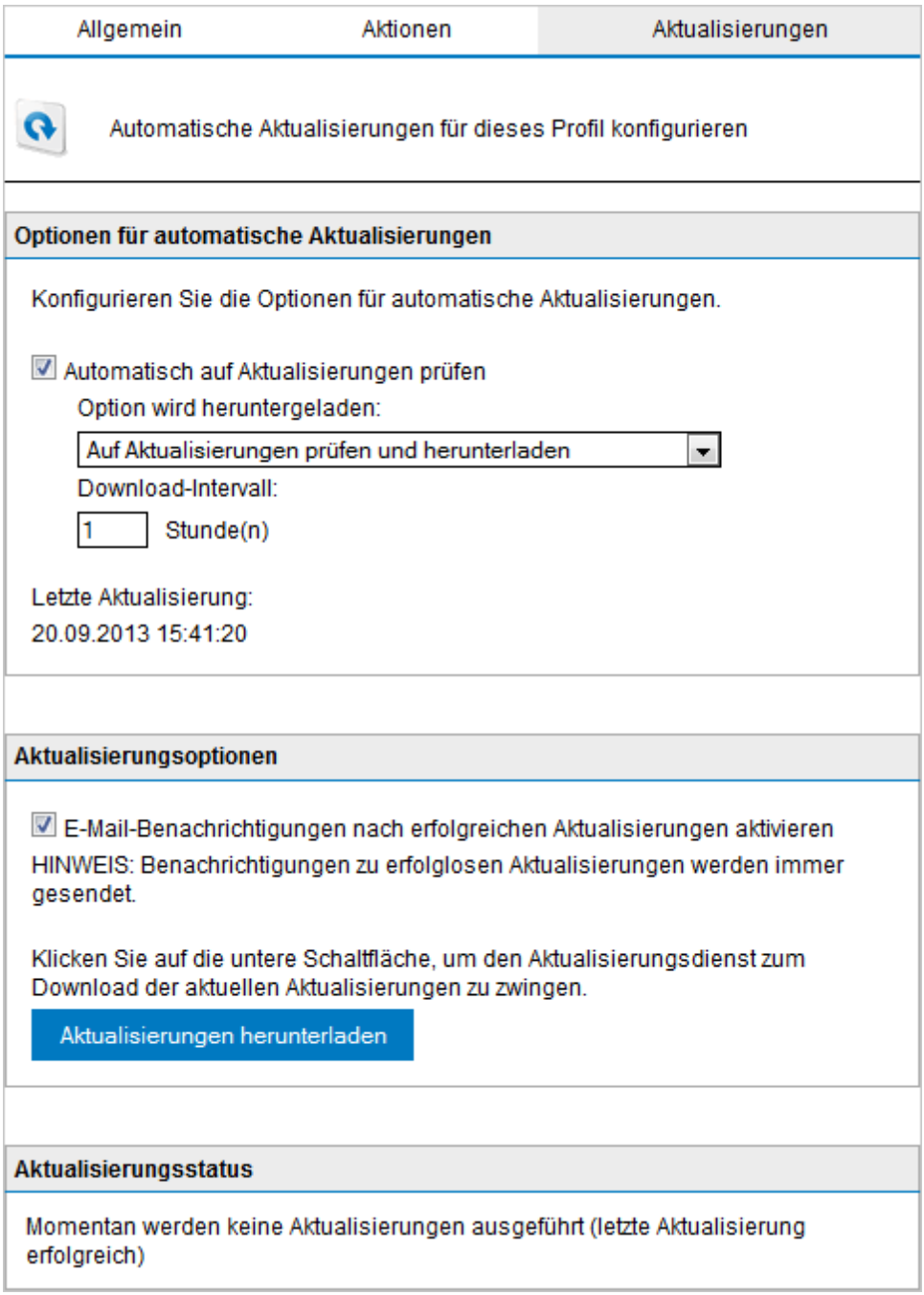
Aktion	Beschreibung
E-Mail in Quarantäne verschieben	Speichert alle infizierten E-Mails, die von der ausgewählten Virenscan-Engine erkannt werden, im Quarantänespeicher. Danach können Sie alle E-Mails in der Quarantäne überprüfen (zulassen/löschen). Weitere Informationen finden Sie unter „Quarantäne“ (Seite 208).
E-Mail löschen	Löscht infizierte E-Mails
Eine bereinigte Kopie der Original-E-Mail in die Empfänger senden	Wählen Sie aus, ob eine bereinigte Kopie der blockierten E-Mail an die Empfänger gesendet werden soll.

7. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

8. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log



Screenshot 41: Aktualisierungen für Virenscan-Engines

9. Wählen Sie auf der Registerkarte **Aktualisierungen** die Option **Automatisch auf Aktualisierungen prüfen** aus, um die automatische Aktualisierung der Anti-Virus-Dateien für die ausgewählte Engine zu aktivieren.

10. Wählen Sie in der Liste **Download-Option** eine der folgenden Optionen aus:

Option	Beschreibung
Nur auf Aktualisierungen prüfen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach Aktualisierungen suchen und den Administrator benachrichtigen soll, sobald Aktualisierungen für diese Engine verfügbar sind. Mit dieser Option werden die verfügbaren Aktualisierungen NICHT automatisch heruntergeladen.
Auf Aktualisierungen prüfen und herunterladen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach verfügbaren Aktualisierungen für diese Engine suchen und diese automatisch herunterladen soll.

11. Geben Sie in Form eines Stundenintervalls an, wie oft GFI MailEssentials nach Aktualisierungen für diese Engine suchen bzw. diese herunterladen soll.

12. Wählen Sie im Bereich **Aktualisierungsoptionen** die Option **E-Mail-Benachrichtigungen nach erfolgreichen Aktualisierungen aktivieren**, um eine Benachrichtigung an den Administrator zu senden, wenn die Engine erfolgreich aktualisiert wurde.

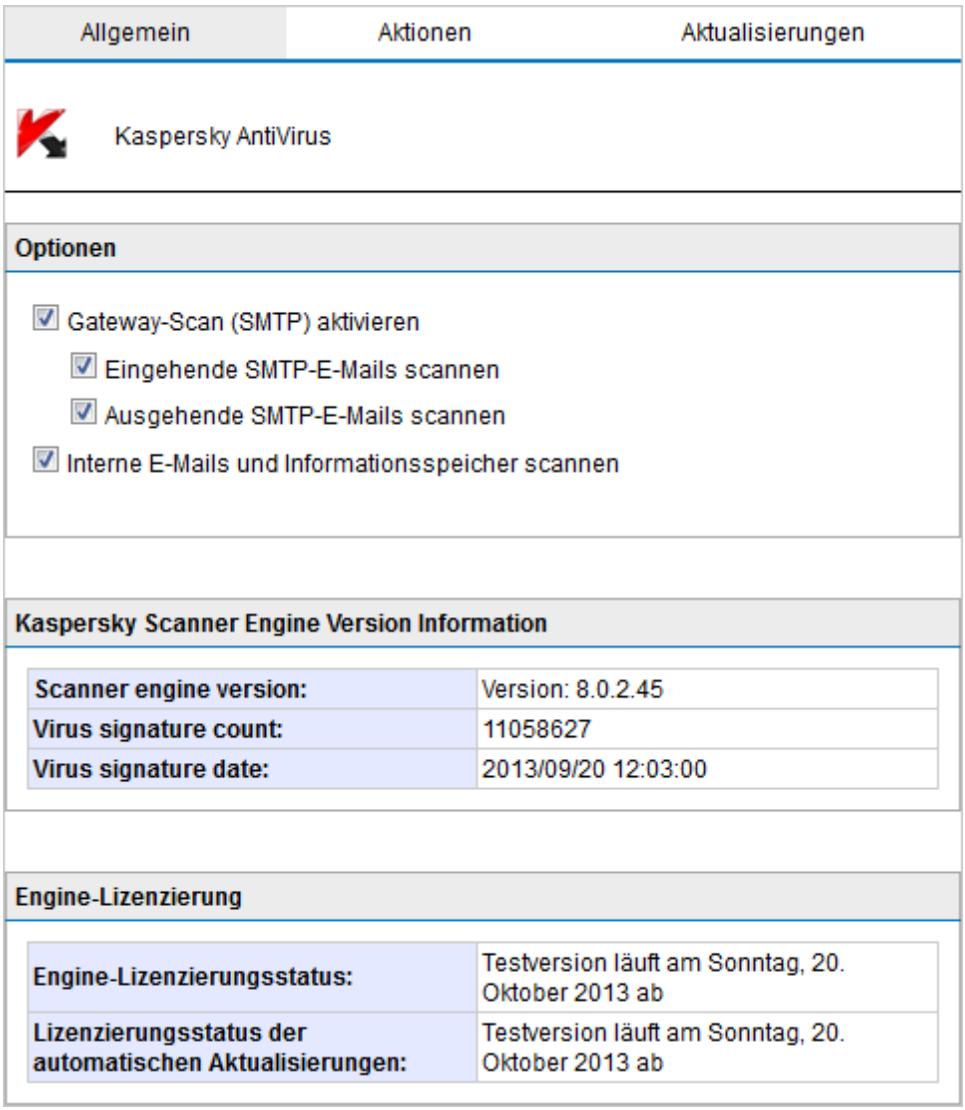
> **HINWEIS**
>
> Wenn Aktualisierungen fehlschlagen, wird immer eine E-Mail-Benachrichtigung gesendet.

13. Klicken Sie auf **Aktualisierungen herunterladen**, um sofort nach Aktualisierungen zu suchen und diese herunterzuladen.

14. Klicken Sie auf **Übernehmen**.

5.1.3 Kaspersky

1. Wählen Sie **E-Mail-Sicherheit > Virenscan-Engines > Kaspersky** aus.



Screenshot 42: Konfiguration von Kaspersky

2. Aktivieren Sie das Kontrollkästchen **Gateway-Scan (SMTP) aktivieren**, um E-Mails mit dieser Virenscan-Engine zu prüfen.

3. Wählen Sie aus, ob eingehende und/oder ausgehende E-Mails mit dieser Virenscan-Engine gescannt werden sollen.

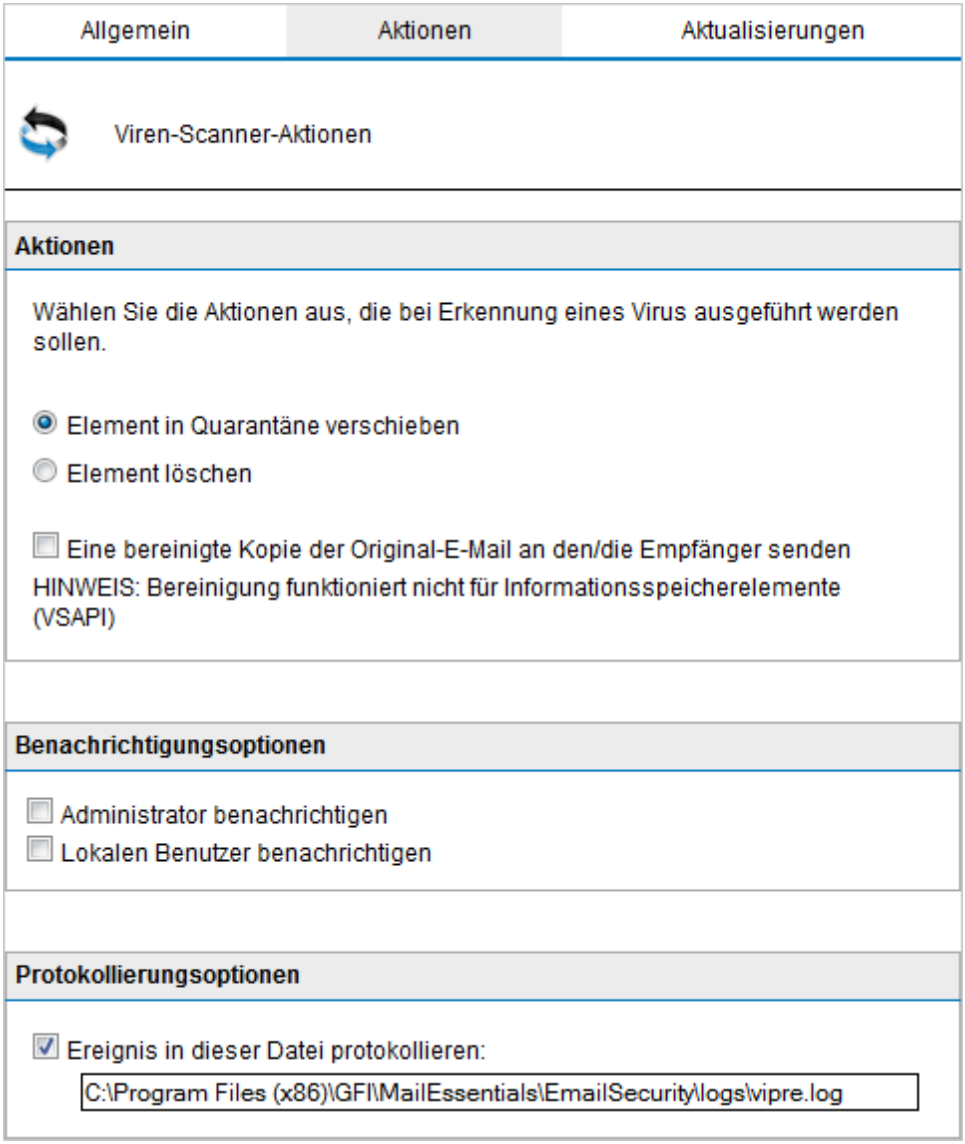
Option	Beschreibung
Eingehende SMTP-E-Mails scannen	Wählen Sie diese Option aus, um eingehende E-Mails zu scannen.
Ausgehende SMTP-E-Mails scannen	Wählen Sie diese Option aus, um ausgehende E-Mails zu scannen.

4. Wenn Sie GFI MailEssentials auf einem Microsoft® Exchange-Rechner installiert haben, können Sie auch interne E-Mails und den Informationsspeicher scannen. Wählen Sie **Interne E-Mails und Informationsspeicherelemente scannen** aus.

> **HINWEIS**
>
> Um den Virenscan des Informationsspeichers zu verwenden, müssen Sie die Option im Knoten **Informationsspeicherschutz** aktivieren. Weitere Informationen finden Sie unter „Informationsspeicherschutz“ (Seite 96).

HINWEIS

Auf dieser Seite können Sie auch die Lizenz- und Versionsinformationen der Anti-Virus-Engine überprüfen.



Screenshot 43: Aktionen der Virenscan-Engine

5. Wählen Sie auf der Registerkarte **Aktionen** aus, was geschehen soll, wenn eine E-Mail blockiert wird:

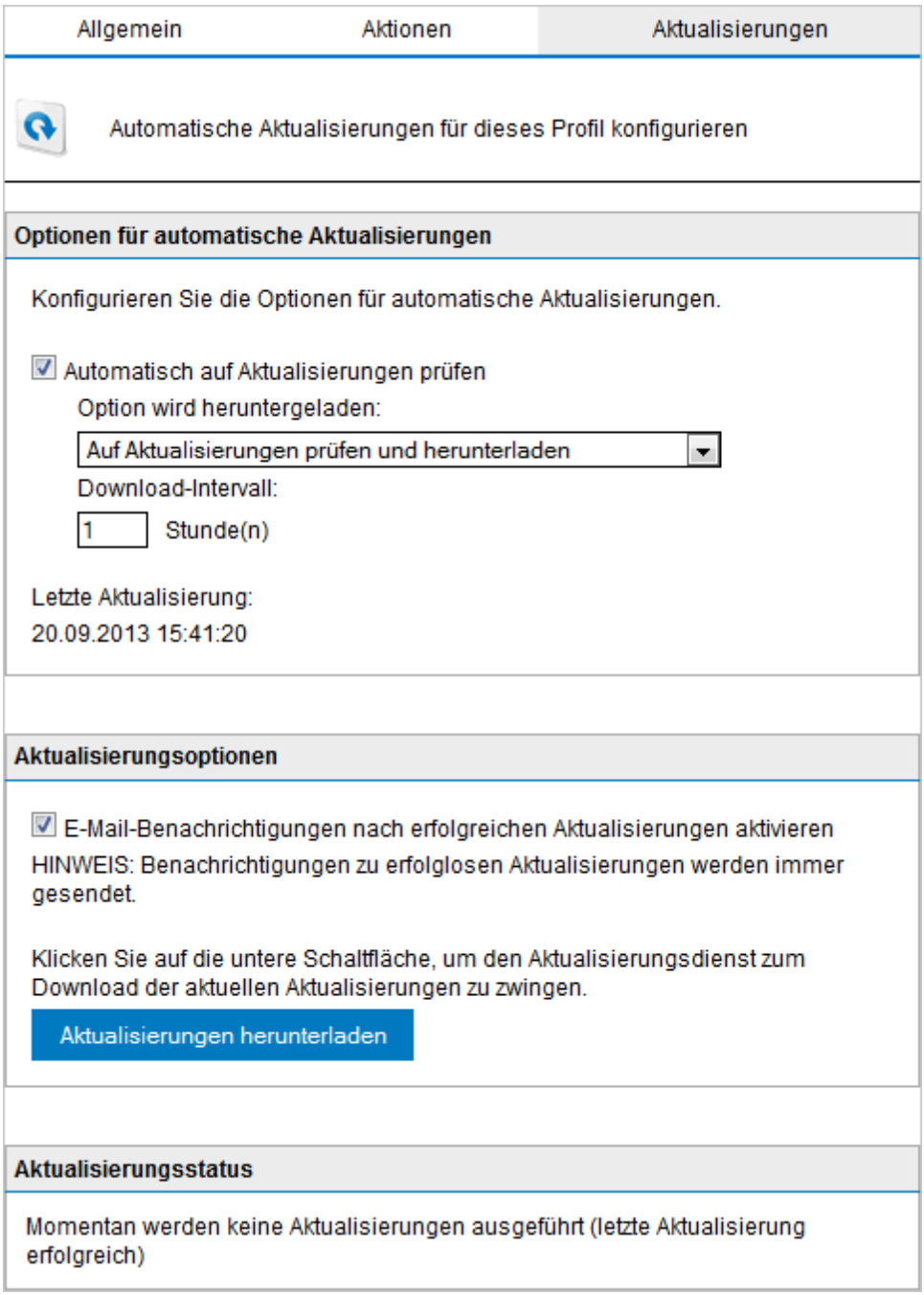
Aktion	Beschreibung
E-Mail in Quarantäne verschieben	Speichert alle infizierten E-Mails, die von der ausgewählten Virenscan-Engine erkannt werden, im Quarantänespeicher. Danach können Sie alle E-Mails in der Quarantäne überprüfen (zulassen/löschen). Weitere Informationen finden Sie unter „Quarantäne“ (Seite 208).
E-Mail löschen	Löscht infizierte E-Mails
Eine bereinigte Kopie der Original-E-Mail in die Empfänger senden	Wählen Sie aus, ob eine bereinigte Kopie der blockierten E-Mail an die Empfänger gesendet werden soll.

6. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

7. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

`<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log`



Screenshot 44: Aktualisierungen für Virenscan-Engines

8. Wählen Sie auf der Registerkarte **Aktualisierungen** die Option **Automatisch auf Aktualisierungen prüfen** aus, um die automatische Aktualisierung der Anti-Virus-Dateien für die ausgewählte Engine zu aktivieren.

9. Wählen Sie in der Liste **Download-Option** eine der folgenden Optionen aus:

Option	Beschreibung
Nur auf Aktualisierungen prüfen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach Aktualisierungen suchen und den Administrator benachrichtigen soll, sobald Aktualisierungen für diese Engine verfügbar sind. Mit dieser Option werden die verfügbaren Aktualisierungen NICHT automatisch heruntergeladen.
Auf Aktualisierungen prüfen und herunterladen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach verfügbaren Aktualisierungen für diese Engine suchen und diese automatisch herunterladen soll.

10. Geben Sie in Form eines Stundenintervalls an, wie oft GFI MailEssentials nach Aktualisierungen für diese Engine suchen bzw. diese herunterladen soll.

11. Wählen Sie im Bereich **Aktualisierungsoptionen** die Option **E-Mail-Benachrichtigungen nach erfolgreichen Aktualisierungen aktivieren**, um eine Benachrichtigung an den Administrator zu senden, wenn die Engine erfolgreich aktualisiert wurde.

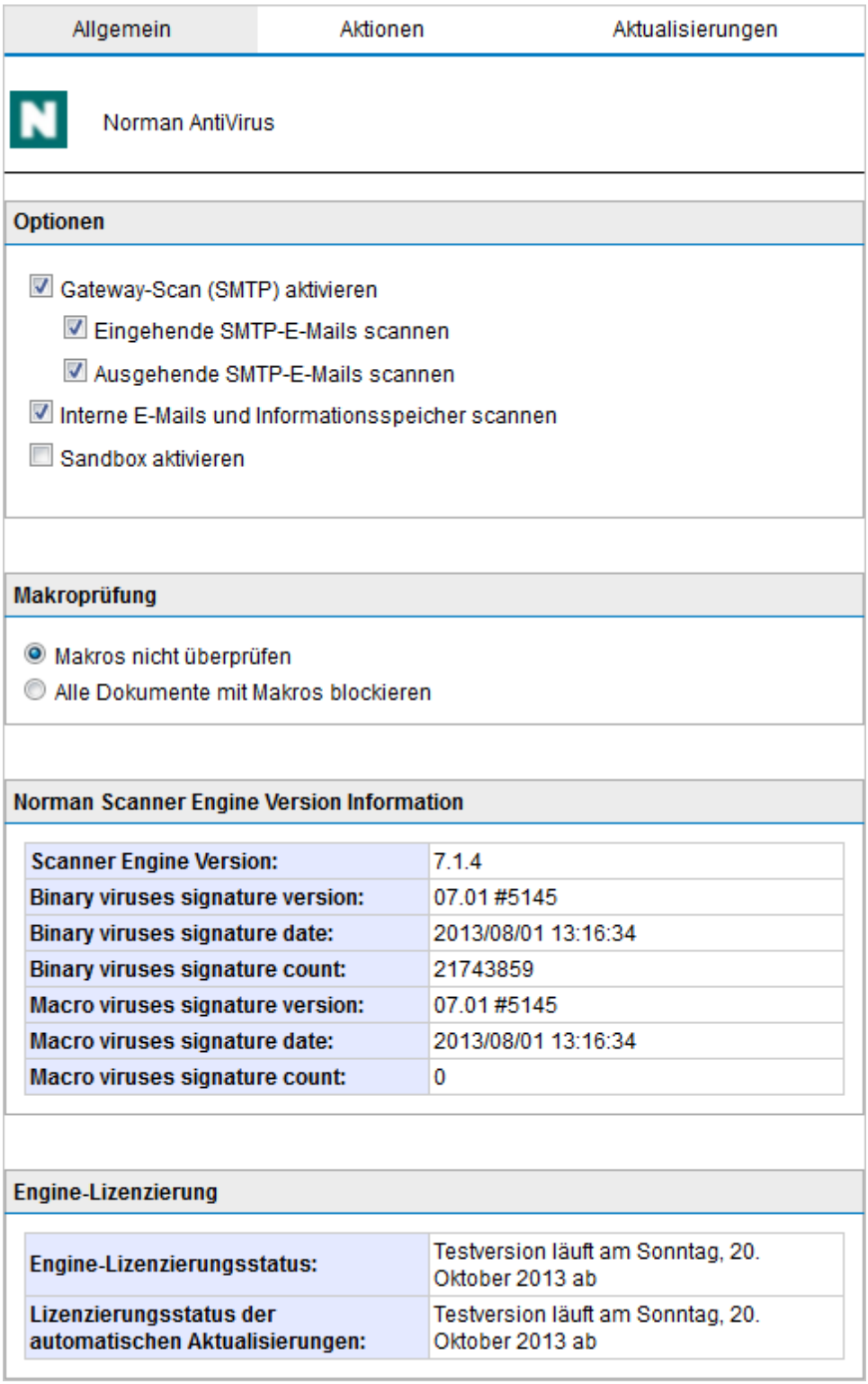
> **HINWEIS**
>
> Wenn Aktualisierungen fehlschlagen, wird immer eine E-Mail-Benachrichtigung gesendet.

12. Klicken Sie auf **Aktualisierungen herunterladen**, um sofort nach Aktualisierungen zu suchen und diese herunterzuladen.

13. Klicken Sie auf **Übernehmen**.

5.1.4 Norman

1. Wählen Sie **E-Mail-Sicherheit > Virenscan-Engines > Norman** aus.


Allgemein
Aktionen
Aktualisierungen
Norman AntiVirus
Optionen
Gateway-Scan (SMTP) aktivieren
Eingehende SMTP-E-Mails scannen
Ausgehende SMTP-E-Mails scannen
Interne E-Mails und Informationsspeicher scannen
Sandbox aktivieren
Makroprüfung
Makros nicht überprüfen
Alle Dokumente mit Makros blockieren
Norman Scanner Engine Version Information
Scanner Engine Version: 7.1.4
Binary viruses signature version: 07.01 #5145
Binary viruses signature date: 2013/08/01 13:16:34
Binary viruses signature count: 21743859
Macro viruses signature version: 07.01 #5145
Macro viruses signature date: 2013/08/01 13:16:34
Macro viruses signature count: 0
Engine-Lizenzierung
Engine-Lizenzierungsstatus: Testversion läuft am Sonntag, 20. Oktober 2013 ab
Lizenzierungsstatus der automatischen Aktualisierungen: Testversion läuft am Sonntag, 20. Oktober 2013 ab

Screenshot 45: Konfiguration von Norman

2. Aktivieren Sie das Kontrollkästchen **Gateway-Scan (SMTP) aktivieren**, um E-Mails mit dieser Virenscan-Engine zu prüfen.

3. Wählen Sie aus, ob eingehende und/oder ausgehende E-Mails mit dieser Virenscan-Engine gescannt werden sollen.

Option	Beschreibung
Eingehende SMTP-E-Mails scannen	Wählen Sie diese Option aus, um eingehende E-Mails zu scannen.
Ausgehende SMTP-E-Mails scannen	Wählen Sie diese Option aus, um ausgehende E-Mails zu scannen.

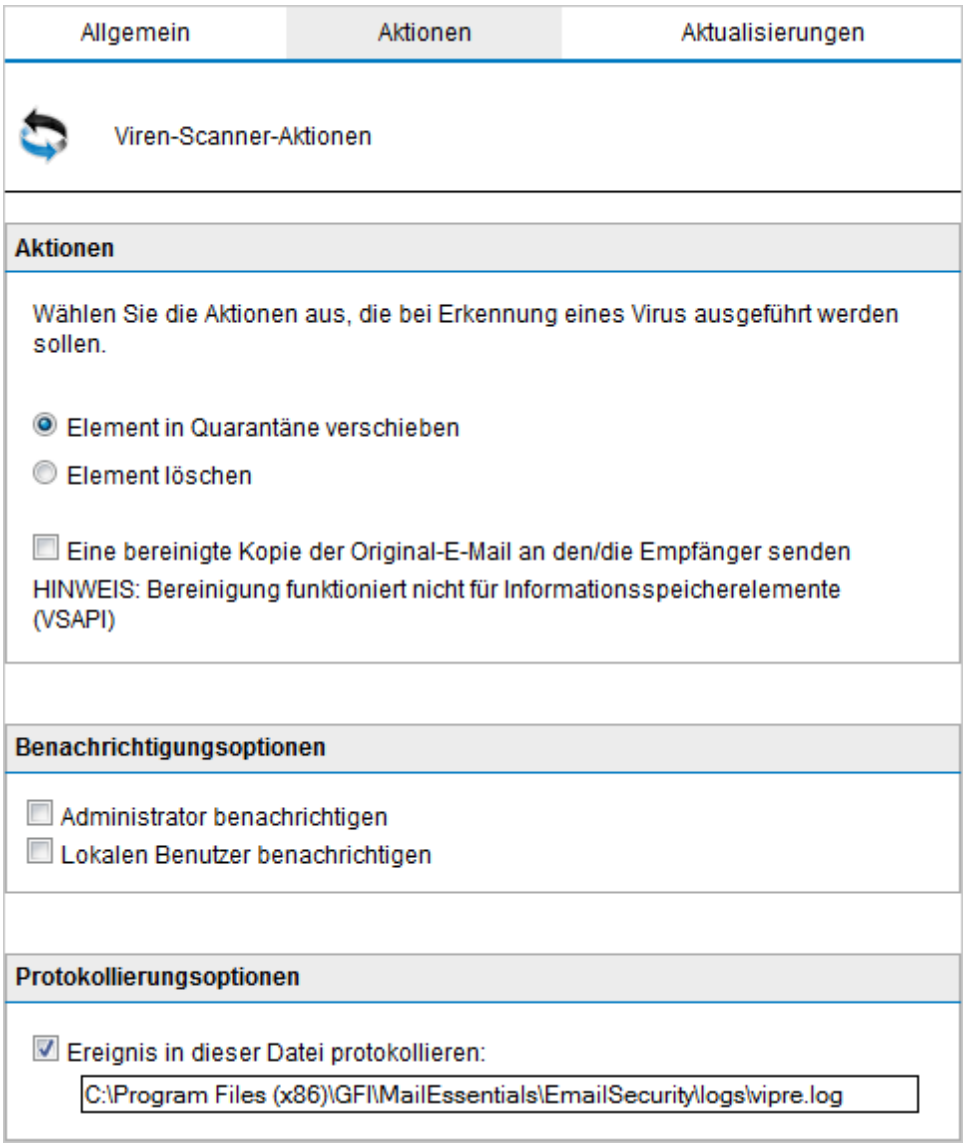
4. Wenn Sie GFI MailEssentials auf einem Microsoft® Exchange-Rechner installiert haben, können Sie auch interne E-Mails und den Informationsspeicher scannen. Wählen Sie **Interne E-Mails und Informationsspeicherelemente scannen** aus.

> **HINWEIS**
>
> Um den Virenscan des Informationsspeichers zu verwenden, müssen Sie die Option im Knoten **Informationsspeicherschutz** aktivieren. Weitere Informationen finden Sie unter „Informationsspeicherschutz“ (Seite 96).

> **HINWEIS**
>
> Auf dieser Seite können Sie auch die Lizenz- und Versionsinformationen der Anti-Virus-Engine überprüfen.

5. Wählen Sie **Sandbox aktivieren** aus, um die Sandbox-Funktion von Norman Antivirus zu verwenden. Diese führt E-Mail-Anhänge in einer virtuellen Umgebung aus und überwacht dabei alle Aktionen und Auswirkungen auf ein System. Zeigt ein Anhang ein virentypisches Verhalten, wird die E-Mail als schädlich markiert, und die entsprechenden Aktionen werden ausgeführt.

> **HINWEIS**
>
> Da diese Prüfung in einer kontrollierten virtuellen Umgebung ausgeführt wird, stellt sie keine Bedrohung für den Computer oder das Netzwerk dar, auf dem GFI MailEssentials installiert ist.



Screenshot 46: Aktionen der Virenscan-Engine

6. Wählen Sie auf der Registerkarte **Aktionen** aus, was geschehen soll, wenn eine E-Mail blockiert wird:

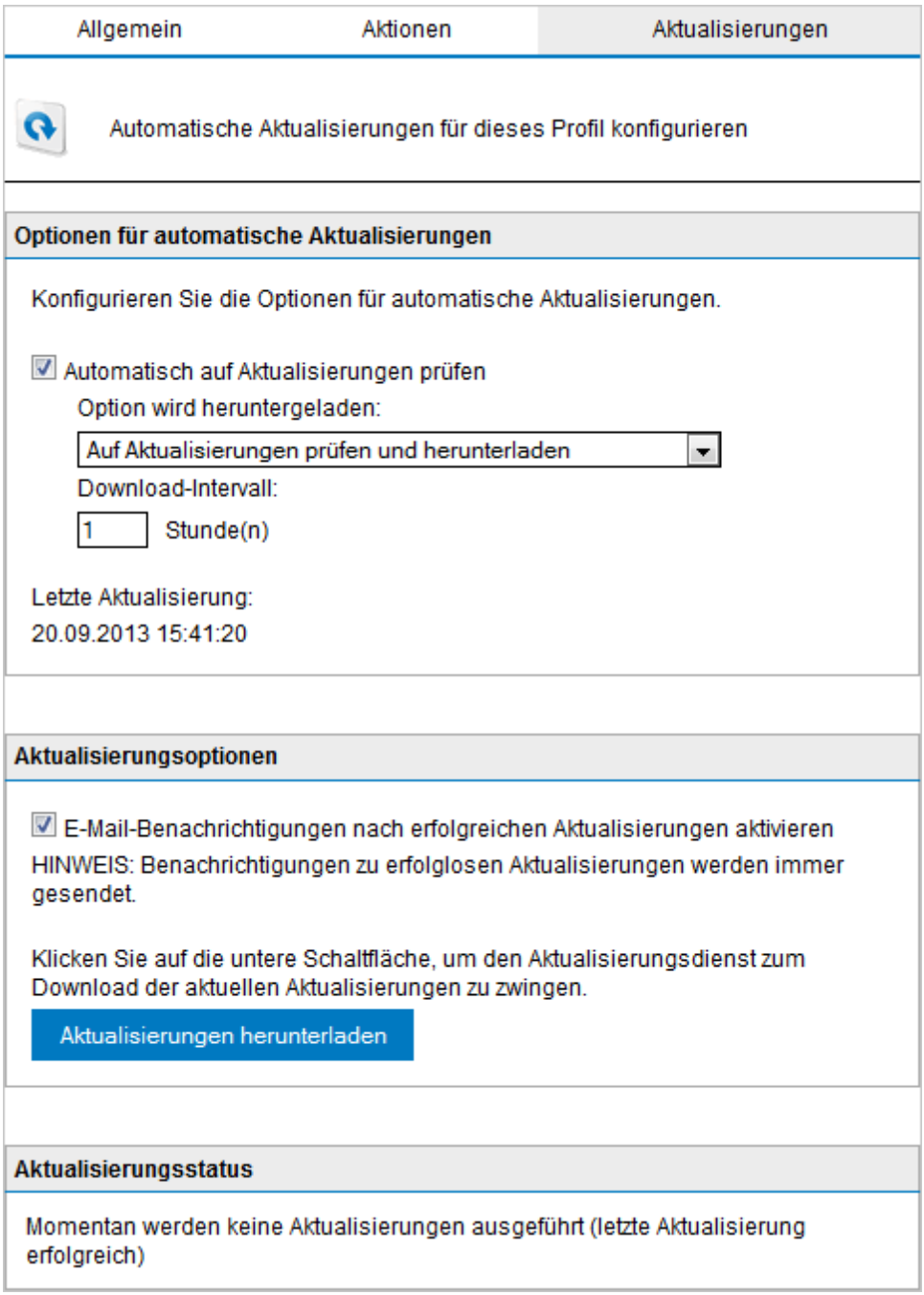
Aktion	Beschreibung
E-Mail in Quarantäne verschieben	Speichert alle infizierten E-Mails, die von der ausgewählten Virenscan-Engine erkannt werden, im Quarantänespeicher. Danach können Sie alle E-Mails in der Quarantäne überprüfen (zulassen/löschen). Weitere Informationen finden Sie unter „Quarantäne“ (Seite 208).
E-Mail löschen	Löscht infizierte E-Mails
Eine bereinigte Kopie der Original-E-Mail in die Empfänger senden	Wählen Sie aus, ob eine bereinigte Kopie der blockierten E-Mail an die Empfänger gesendet werden soll.

7. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

8. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log



Screenshot 47: Aktualisierungen für Virenscan-Engines

9. Wählen Sie auf der Registerkarte **Aktualisierungen** die Option **Automatisch auf Aktualisierungen prüfen** aus, um die automatische Aktualisierung der Anti-Virus-Dateien für die ausgewählte Engine zu aktivieren.

10. Wählen Sie in der Liste **Download-Option** eine der folgenden Optionen aus:

Option	Beschreibung
Nur auf Aktualisierungen prüfen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach Aktualisierungen suchen und den Administrator benachrichtigen soll, sobald Aktualisierungen für diese Engine verfügbar sind. Mit dieser Option werden die verfügbaren Aktualisierungen NICHT automatisch heruntergeladen.
Auf Aktualisierungen prüfen und herunterladen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach verfügbaren Aktualisierungen für diese Engine suchen und diese automatisch herunterladen soll.

11. Geben Sie in Form eines Stundenintervalls an, wie oft GFI MailEssentials nach Aktualisierungen für diese Engine suchen bzw. diese herunterladen soll.

12. Wählen Sie im Bereich **Aktualisierungsoptionen** die Option **E-Mail-Benachrichtigungen nach erfolgreichen Aktualisierungen aktivieren**, um eine Benachrichtigung an den Administrator zu senden, wenn die Engine erfolgreich aktualisiert wurde.

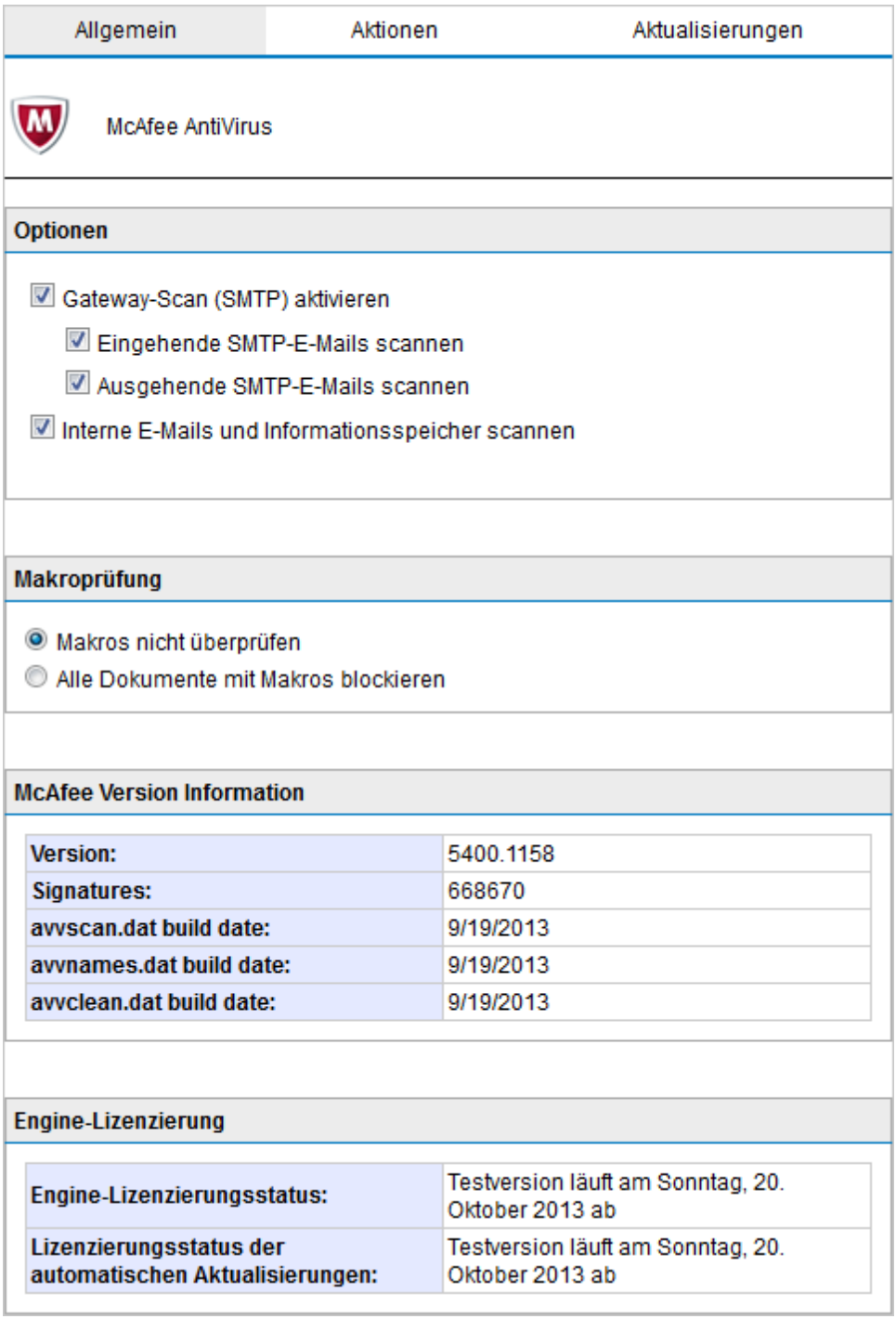
> **HINWEIS**
>
> Wenn Aktualisierungen fehlschlagen, wird immer eine E-Mail-Benachrichtigung gesendet.

13. Klicken Sie auf **Aktualisierungen herunterladen**, um sofort nach Aktualisierungen zu suchen und diese herunterzuladen.

14. Klicken Sie auf **Übernehmen**.

5.1.5 McAfee

1. Wählen Sie **E-Mail-Sicherheit > Virenscan-Engines > McAfee** aus.



Screenshot 48: Konfiguration von McAfee

2. Aktivieren Sie das Kontrollkästchen **Gateway-Scan (SMTP) aktivieren**, um E-Mails mit dieser Virenscan-Engine zu prüfen.

3. Wählen Sie aus, ob eingehende und/oder ausgehende E-Mails mit dieser Virenscan-Engine gescannt werden sollen.

Option	Beschreibung
Eingehende SMTP-E-Mails scannen	Wählen Sie diese Option aus, um eingehende E-Mails zu scannen.
Ausgehende SMTP-E-Mails scannen	Wählen Sie diese Option aus, um ausgehende E-Mails zu scannen.

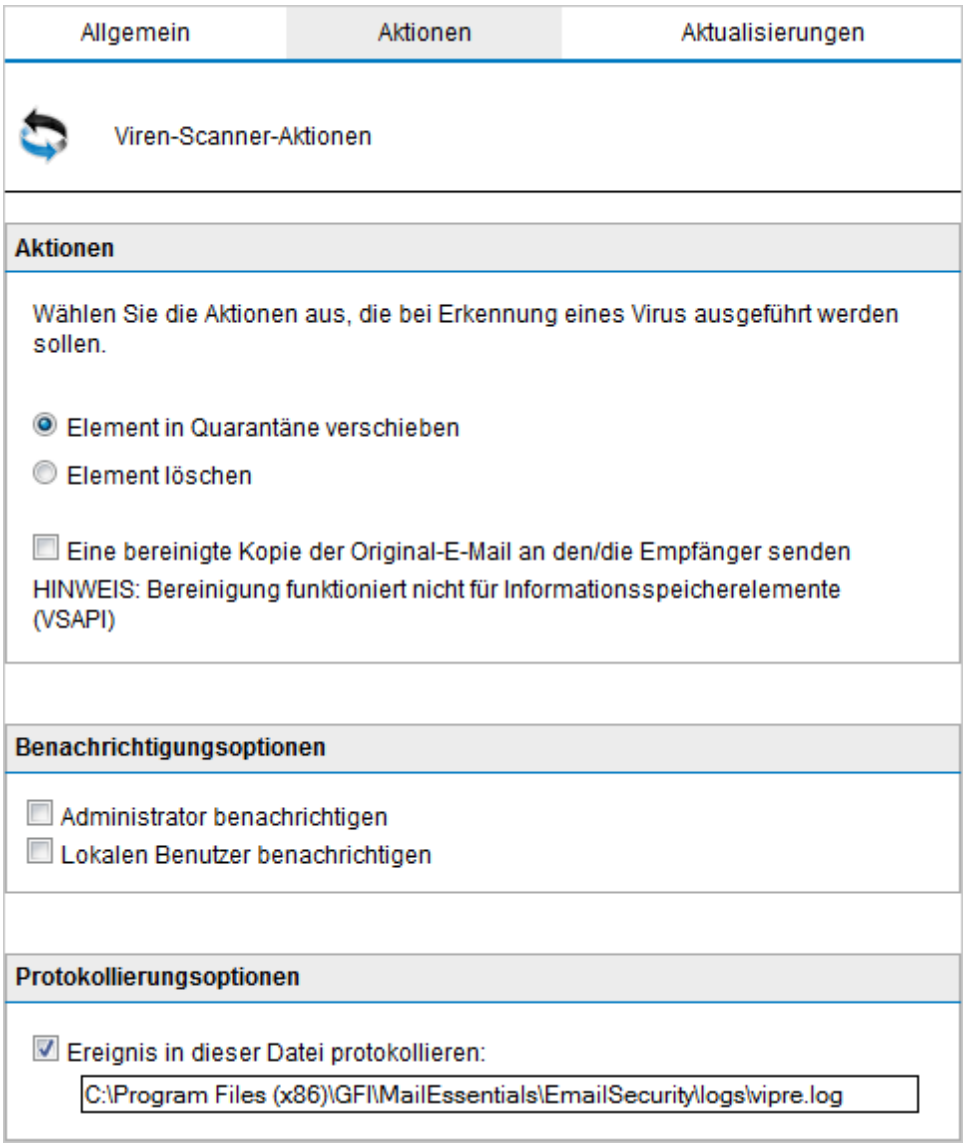
4. Wenn Sie GFI MailEssentials auf einem Microsoft® Exchange-Rechner installiert haben, können Sie auch interne E-Mails und den Informationsspeicher scannen. Wählen Sie **Interne E-Mails und**

Informationsspeicherelemente scannen aus.

> **HINWEIS**
>
> Um den Virenscan des Informationsspeichers zu verwenden, müssen Sie die Option im Knoten **Informationsspeicherschutz** aktivieren. Weitere Informationen finden Sie unter „Informationsspeicherschutz“ (Seite 96).

> **HINWEIS**
>
> Auf dieser Seite können Sie auch die Lizenz- und Versionsinformationen der Anti-Virus-Engine überprüfen.

5. Mit McAfee Antivirus können auch E-Mails mit Anhängen blockiert werden, die Makros enthalten. Sie aktivieren diese Funktion, indem Sie im Bereich **Makroprüfung** die Option **Alle Dokumente mit Makros blockieren** auswählen.



Screenshot 49: Aktionen der Virenscan-Engine

6. Wählen Sie auf der Registerkarte **Aktionen** aus, was geschehen soll, wenn eine E-Mail blockiert wird:

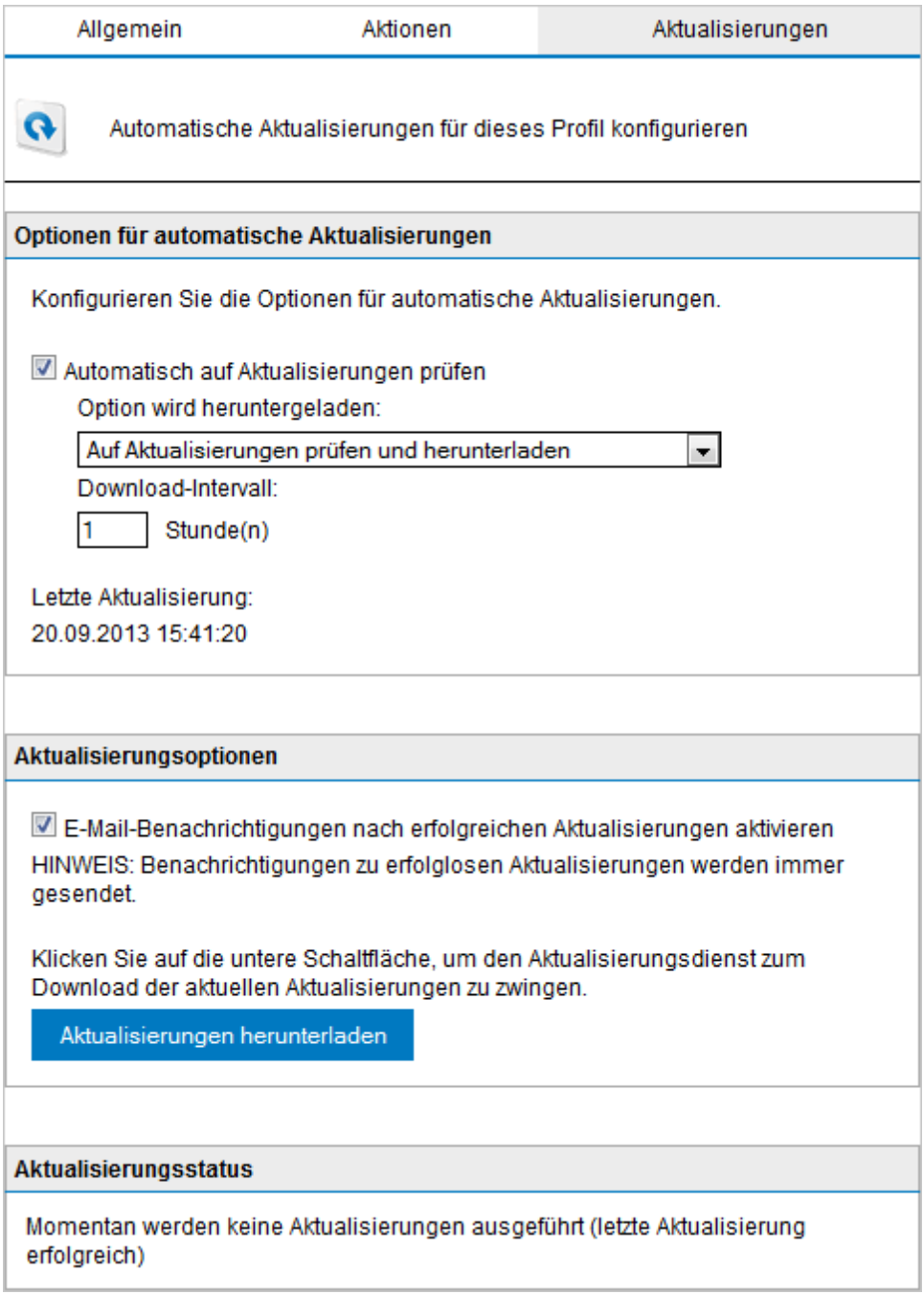
Aktion	Beschreibung
E-Mail in Quarantäne verschieben	Speichert alle infizierten E-Mails, die von der ausgewählten Virenscan-Engine erkannt werden, im Quarantänespeicher. Danach können Sie alle E-Mails in der Quarantäne überprüfen (zulassen/löschen). Weitere Informationen finden Sie unter „Quarantäne“ (Seite 208).
E-Mail löschen	Löscht infizierte E-Mails
Eine bereinigte Kopie der Original-E-Mail in die Empfänger senden	Wählen Sie aus, ob eine bereinigte Kopie der blockierten E-Mail an die Empfänger gesendet werden soll.

7. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

8. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

```
<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log
```



Screenshot 50: Aktualisierungen für Virenscan-Engines

9. Wählen Sie auf der Registerkarte **Aktualisierungen** die Option **Automatisch auf Aktualisierungen prüfen** aus, um die automatische Aktualisierung der Anti-Virus-Dateien für die ausgewählte Engine zu aktivieren.

10. Wählen Sie in der Liste **Download-Option** eine der folgenden Optionen aus:

Option	Beschreibung
Nur auf Aktualisierungen prüfen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach Aktualisierungen suchen und den Administrator benachrichtigen soll, sobald Aktualisierungen für diese Engine verfügbar sind. Mit dieser Option werden die verfügbaren Aktualisierungen NICHT automatisch heruntergeladen.
Auf Aktualisierungen prüfen und herunterladen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach verfügbaren Aktualisierungen für diese Engine suchen und diese automatisch herunterladen soll.

11. Geben Sie in Form eines Stundenintervalls an, wie oft GFI MailEssentials nach Aktualisierungen für diese Engine suchen bzw. diese herunterladen soll.

12. Wählen Sie im Bereich **Aktualisierungsoptionen** die Option **E-Mail-Benachrichtigungen nach erfolgreichen Aktualisierungen aktivieren**, um eine Benachrichtigung an den Administrator zu senden, wenn die Engine erfolgreich aktualisiert wurde.

> **HINWEIS**
>
> Wenn Aktualisierungen fehlschlagen, wird immer eine E-Mail-Benachrichtigung gesendet.

13. Klicken Sie auf **Aktualisierungen herunterladen**, um sofort nach Aktualisierungen zu suchen und diese herunterzuladen.

14. Klicken Sie auf **Übernehmen**.

5.2 Informationsspeicherschutz

Ist GFI MailEssentials auf dem Microsoft® Exchange-Server installiert, ermöglicht der Informationsspeicherschutz einen Virenscan des Microsoft® Exchange-Informationsspeichers durch die Virenscan-Engines.

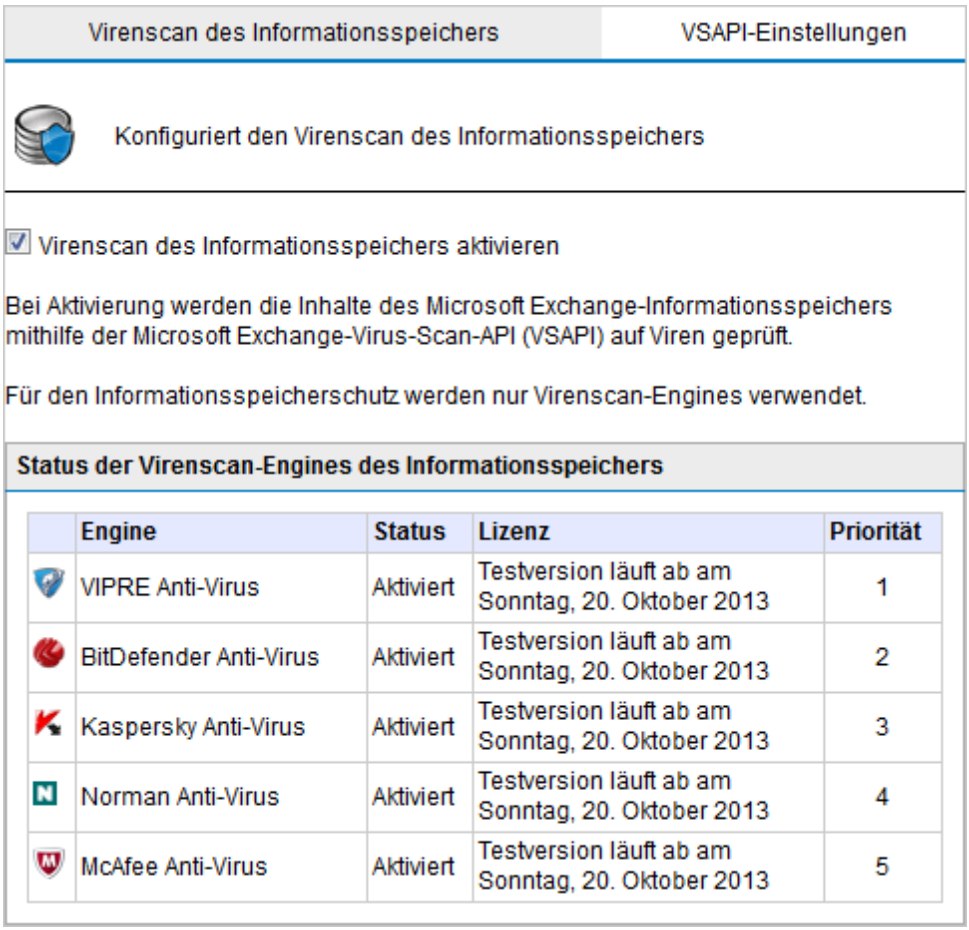
> **HINWEIS**
>
> Ist GFI MailEssentials auf einem Rechner mit Microsoft® Exchange Server 2007/2010 installiert, ist der Informationsspeicherschutz nur verfügbar, wenn sowohl die Postfachserverrolle als auch die Hub-Transport-Serverrolle installiert sind.

> **HINWEIS**
>
> Informationsspeicherschutz (VSAPI) wird unter Microsoft® Exchange Server 2013 nicht unterstützt, da Microsoft VSAPI von Microsoft® Exchange Server 2013 entfernt hat.

In diesem Abschnitt wird beschrieben, wie Sie den Scan des Informationsspeichers aktivieren und die Scanmethode auswählen, die von der Virus Scanning API (VSAPI) verwendet werden soll.

5.2.1 Scan des Informationsspeichers

1. Wählen Sie **E-Mail-Sicherheit > Informationsspeicherschutz** aus.



Screenshot 51: Knoten für den Informationsspeicherschutz

2. Wählen Sie auf der Registerkarte **Virenscan des Informationsspeichers** die Option **Virenscan des Informationsspeichers aktivieren** aus.

3. Klicken Sie auf **Übernehmen**.

Der Status der Virenscan-Engines, die für den Scan des Informationsspeichers verwendet werden, wird in der Tabelle angezeigt.

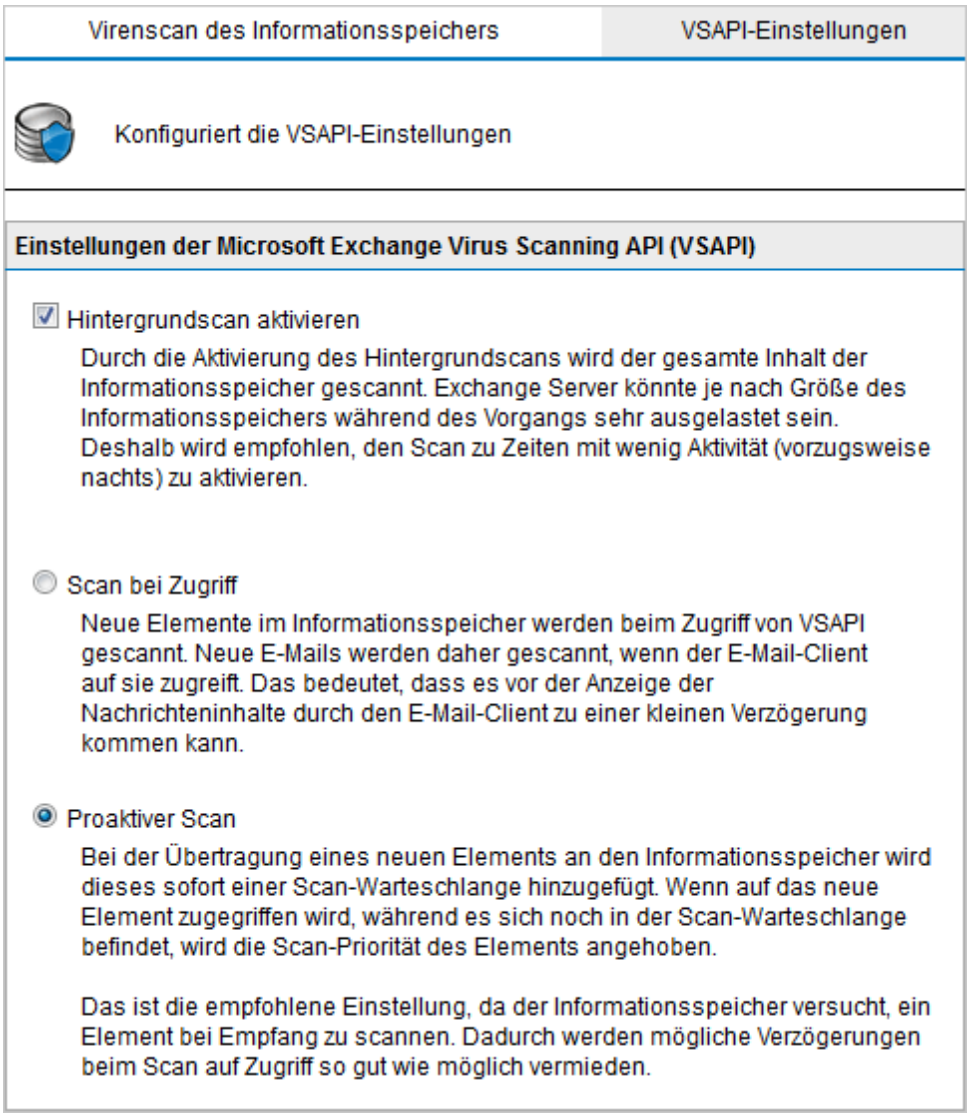
Sie können auch einzelne Virenscan-Engines für den Scan des Informationsspeichers deaktivieren. Öffnen Sie die Seite der Virenscan-Engines, wählen Sie die gewünschte Engine aus, und deaktivieren Sie die Option **Interne E-Mails und Informationsspeicherelemente scannen**.

5.2.2 VSAPI-Einstellungen

Die Methode, die GFI MailEssentials für den Zugriff auf E-Mails und Anhänge im Microsoft® Exchange-Informationsspeicher verwendet, ist die VSAPI (Virus Scanning Application Programming Interface). GFI MailEssentials bietet die Möglichkeit, die gewünschte Scanmethode für den Informationsspeicher festzulegen.

1. Wählen Sie **E-Mail-Sicherheit > Informationsspeicherschutz** aus.

2. Wählen Sie die Registerkarte **VSAPI-Einstellungen** aus.


Virenscan des Informationsspeichers
VSAPI-Einstellungen
Konfiguriert die VSAPI-Einstellungen
Einstellungen der Microsoft Exchange Virus Scanning API (VSAPI)
Hintergrundscan aktivieren
Durch die Aktivierung des Hintergrundscans wird der gesamte Inhalt der Informationsspeicher gescannt. Exchange Server könnte je nach Größe des Informationsspeichers während des Vorgangs sehr ausgelastet sein. Deshalb wird empfohlen, den Scan zu Zeiten mit wenig Aktivität (vorzugsweise nachts) zu aktivieren.
Scan bei Zugriff
Neue Elemente im Informationsspeicher werden beim Zugriff von VSAPI gescannt. Neue E-Mails werden daher gescannt, wenn der E-Mail-Client auf sie zugreift. Das bedeutet, dass es vor der Anzeige der Nachrichteninhalte durch den E-Mail-Client zu einer kleinen Verzögerung kommen kann.
Proaktiver Scan
Bei der Übertragung eines neuen Elements an den Informationsspeicher wird dieses sofort einer Scan-Warteschlange hinzugefügt. Wenn auf das neue Element zugegriffen wird, während es sich noch in der Scan-Warteschlange befindet, wird die Scan-Priorität des Elements angehoben.
Das ist die empfohlene Einstellung, da der Informationsspeicher versucht, ein Element bei Empfang zu scannen. Dadurch werden mögliche Verzögerungen beim Scan auf Zugriff so gut wie möglich vermieden.

Screenshot 52: VSAPI-Einstellungen

3. Wählen Sie bei Bedarf die Option **Hintergrundscan aktivieren** aus, um den Scan des Informationsspeichers im Hintergrund auszuführen (optional).

WARNHINWEIS

Beim Hintergrundscan wird der gesamte Inhalt des Informationsspeichers gescannt. Dies kann – abhängig von der Anzahl der Elemente im Informationsspeicher – zu einer hohen Systembelastung des Microsoft® Exchange-Servers führen. Es wird daher empfohlen, diese Option nur für Zeiträume mit geringer Serveraktivität (z. B. nachts) zu aktivieren.

4. Wählen Sie eine VSAPI-Scanmethode aus:

Scanmethode	Beschreibung
Scan bei Zugriff	Neue Elemente im Informationsspeicher werden beim Zugriff durch den E-Mail-Client gescannt. Das bedeutet, dass es vor der Anzeige der Nachrichteninhalte durch den E-Mail-Client zu einer kleinen Verzögerung kommen kann.

Scanmethode	Beschreibung
Proaktiver Scan	Neue Elemente, die dem Informationsspeicher hinzugefügt werden, werden in eine Scan-Warteschlange eingereiht. Dies ist der empfohlene Standardmodus, da er im Allgemeinen die Verzögerung vermeidet, die der Scan bei Zugriff verursacht. **HINWEIS** Falls ein E-Mail-Client versucht, auf ein Element zuzugreifen, das sich noch in der Warteschlange befindet, erhält dieses eine höhere Scanpriorität und wird somit sofort gescannt.

5. Klicken Sie auf **Übernehmen**.

5.3 Scanner für Trojaner und ausführbare Dateien

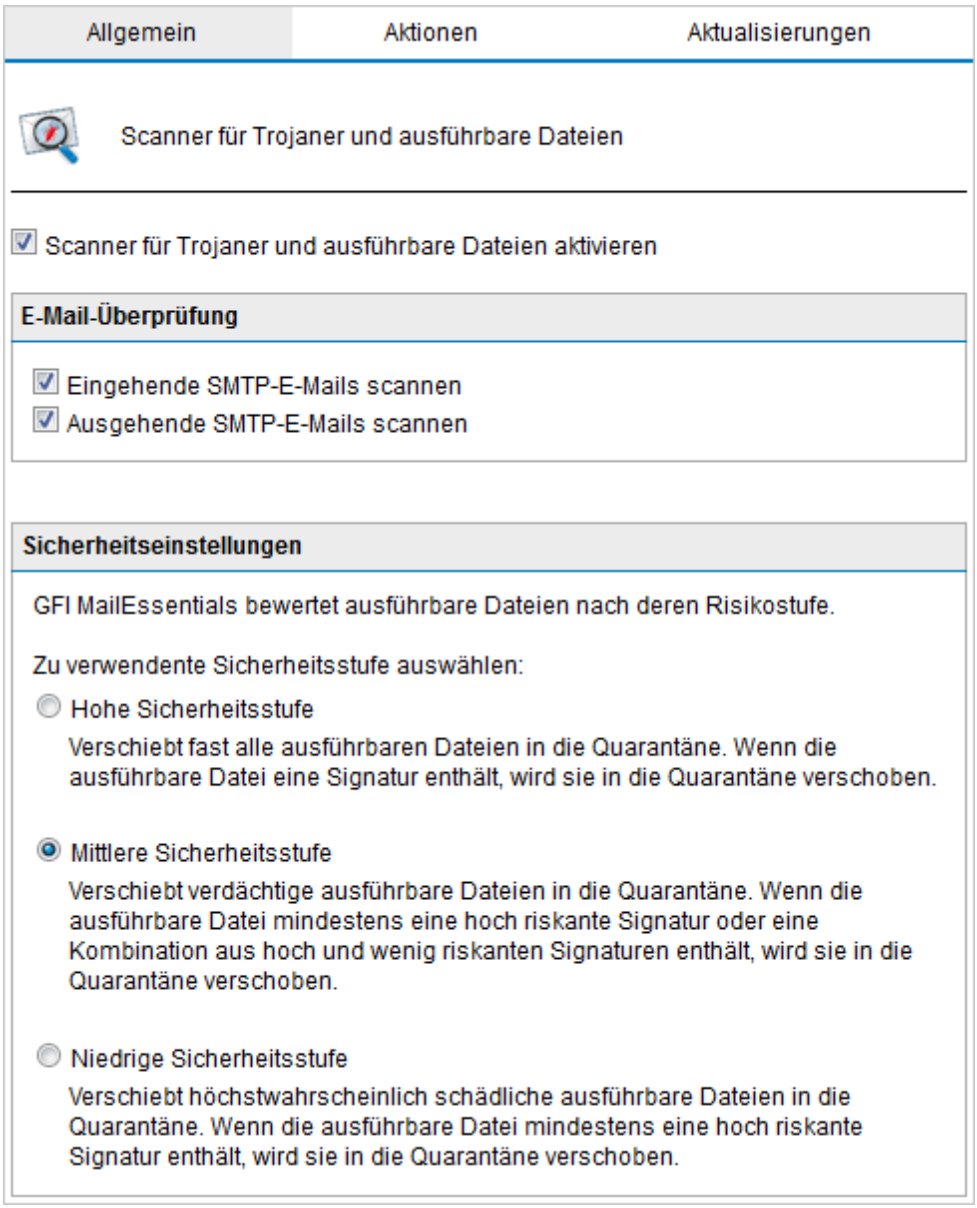
Der Scanner für Trojaner und ausführbare Dateien analysiert und ermittelt die Funktion von ausführbaren Dateien, die an E-Mails angehängt sind. Anschließend kann der Scanner alle ausführbaren Dateien, die verdächtige Aktivitäten durchführen (z. B. Trojaner), in die Quarantäne verschieben.

Wie funktioniert der Scanner für Trojaner und ausführbare Dateien?

GFI MailEssentials bewertet das Risiko, das von einer ausführbaren Datei ausgeht, indem die Datei dekompiliert wird und in Echtzeit erkannt wird, was sie bewirken könnte. Anschließend werden die Funktionen der ausführbaren Datei mit einer Datenbank mit schädlichen Aktionen verglichen, und das Risiko wird bewertet. Mit dem Scanner für Trojaner und ausführbare Dateien können Sie potenziell gefährliche, unbekannte oder einmalige Trojaner erkennen und blockieren, bevor sie Ihr Netzwerk gefährden.

5.3.1 Konfigurieren des Scanners für Trojaner und ausführbare Dateien

1. Wählen Sie **E-Mail-Sicherheit > Scanner für Trojaner und ausführbare Dateien** aus.


Allgemein
Aktionen
Aktualisierungen
Scanner für Trojaner und ausführbare Dateien
Scanner für Trojaner und ausführbare Dateien aktivieren
E-Mail-Überprüfung
Eingehende SMTP-E-Mails scannen
Ausgehende SMTP-E-Mails scannen
Sicherheitseinstellungen
GFI MailEssentials bewertet ausführbare Dateien nach deren Risikostufe.
Zu verwendente Sicherheitsstufe auswählen:
Hohe Sicherheitsstufe
Verschiebt fast alle ausführbaren Dateien in die Quarantäne. Wenn die ausführbare Datei eine Signatur enthält, wird sie in die Quarantäne verschoben.
Mittlere Sicherheitsstufe
Verschiebt verdächtige ausführbare Dateien in die Quarantäne. Wenn die ausführbare Datei mindestens eine hoch riskante Signatur oder eine Kombination aus hoch und wenig riskanten Signaturen enthält, wird sie in die Quarantäne verschoben.
Niedrige Sicherheitsstufe
Verschiebt höchstwahrscheinlich schädliche ausführbare Dateien in die Quarantäne. Wenn die ausführbare Datei mindestens eine hoch riskante Signatur enthält, wird sie in die Quarantäne verschoben.

Screenshot 53: Scanner für Trojaner und ausführbare Dateien: Registerkarte 'Allgemein'

2. Wählen Sie **Scanner für Trojaner und ausführbare Dateien aktivieren** aus, um diesen Filter zu aktivieren.

3. Geben Sie im Bereich **E-Mail-Überprüfung** die E-Mails an, die auf Trojaner und andere schädliche ausführbare Dateien geprüft werden sollen, indem Sie die gewünschten Optionen auswählen:

Option	Beschreibung
Eingehende E-Mails prüfen	Eingehende E-Mails werden auf Trojaner und schädliche ausführbare Dateien geprüft.
Ausgehende E-Mails prüfen	Ausgehende E-Mails werden auf Trojaner und schädliche ausführbare Dateien geprüft.

4. Wählen Sie im Bereich **Sicherheitseinstellungen** die gewünschte Sicherheitsstufe aus:

Sicherheitsstufe	Beschreibung
Hohe Sicherheitsstufe	Blockiert alle ausführbaren Dateien, die bekannte schädliche Signaturen enthalten.
Mittlere Sicherheitsstufe	Blockiert verdächtige ausführbare Dateien E-Mails werden blockiert, wenn eine ausführbare Datei eine hoch riskante Signatur oder eine Kombination aus hoch und wenig riskanten Signaturen enthält.
Niedrige Sicherheitsstufe	Blockiert nur schädliche ausführbare Dateien. E-Mails werden blockiert, wenn eine ausführbare Datei mindestens eine hoch riskante Signatur enthält.

5. Konfigurieren Sie auf der Registerkarte **Aktionen** die Aktionen, die GFI MailEssentials für E-Mails ausführen soll, die eine schädliche ausführbare Datei enthalten.

HINWEIS

E-Mails, die vom Scanner für Trojaner und ausführbare Dateien blockiert werden, werden immer in die Quarantäne verschoben.

HINWEIS

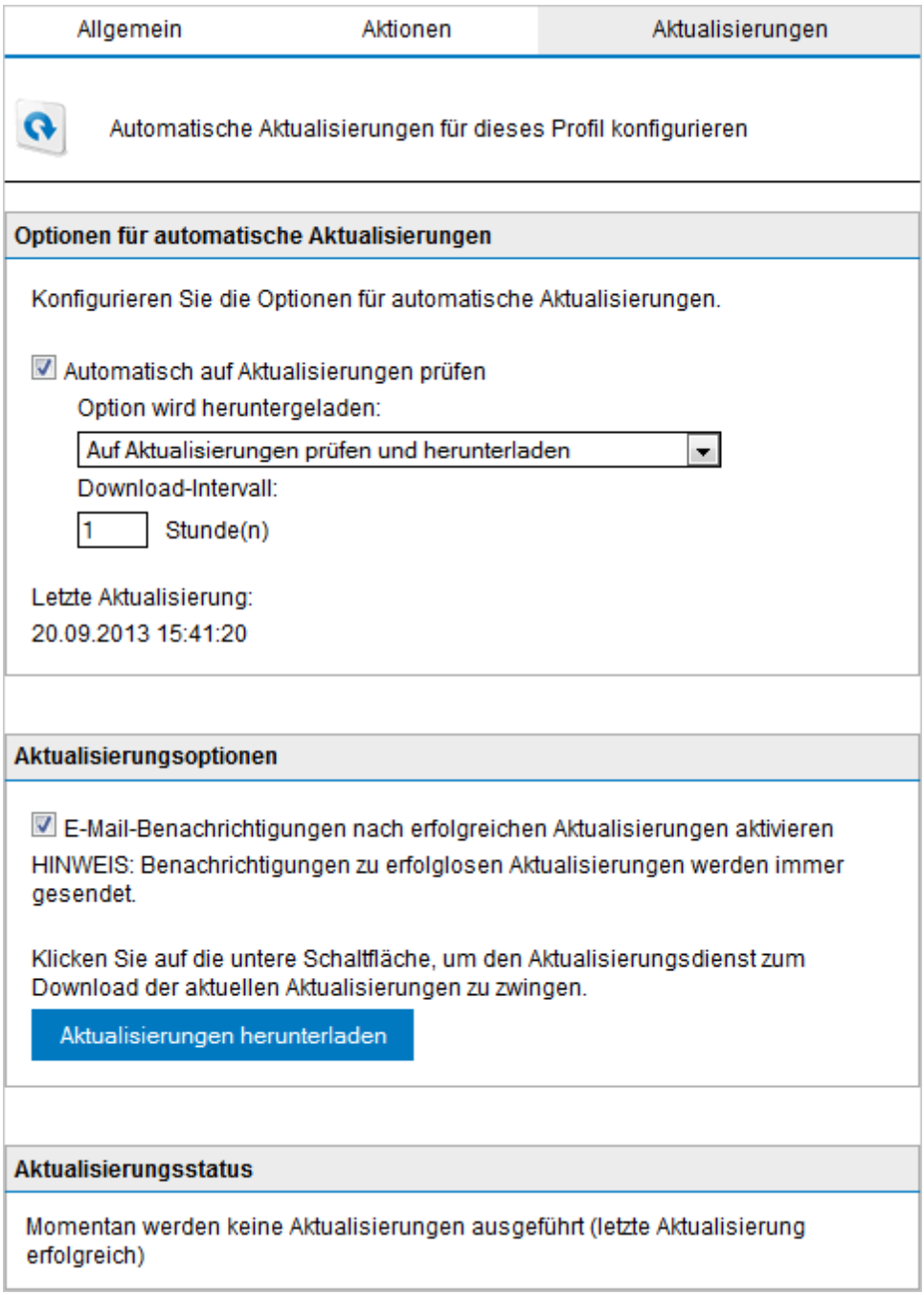
Wenn GFI MailEssentials auf demselben Rechner wie Microsoft® Exchange 2003 installiert wird, kann GFI MailEssentials ausgehende E-Mails möglicherweise nicht blockieren, sondern ersetzt stattdessen den blockierten Inhalt mit einem Bedrohungsbericht.

6. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

7. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

```
<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log
```



Screenshot 54: Aktualisierungen für Virenscan-Engines

8. Wählen Sie auf der Registerkarte **Aktualisierungen** die Option **Automatisch auf Aktualisierungen prüfen** aus, um die automatische Aktualisierung der Anti-Virus-Dateien für die ausgewählte Engine zu aktivieren.

9. Wählen Sie in der Liste **Download-Option** eine der folgenden Optionen aus:

Option	Beschreibung
Nur auf Aktualisierungen prüfen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach Aktualisierungen suchen und den Administrator benachrichtigen soll, sobald Aktualisierungen für diese Engine verfügbar sind. Mit dieser Option werden die verfügbaren Aktualisierungen NICHT automatisch heruntergeladen.
Auf Aktualisierungen prüfen und herunterladen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach verfügbaren Aktualisierungen für diese Engine suchen und diese automatisch herunterladen soll.

10. Geben Sie in Form eines Stundenintervalls an, wie oft GFI MailEssentials nach Aktualisierungen für diese Engine suchen bzw. diese herunterladen soll.

11. Wählen Sie im Bereich **Aktualisierungsoptionen** die Option **E-Mail-Benachrichtigungen nach erfolgreichen Aktualisierungen aktivieren**, um eine Benachrichtigung an den Administrator zu senden, wenn die Engine erfolgreich aktualisiert wurde.

> **HINWEIS**
>
> Wenn Aktualisierungen fehlschlagen, wird immer eine E-Mail-Benachrichtigung gesendet.

12. Klicken Sie auf **Aktualisierungen herunterladen**, um sofort nach Aktualisierungen zu suchen und diese herunterzuladen.

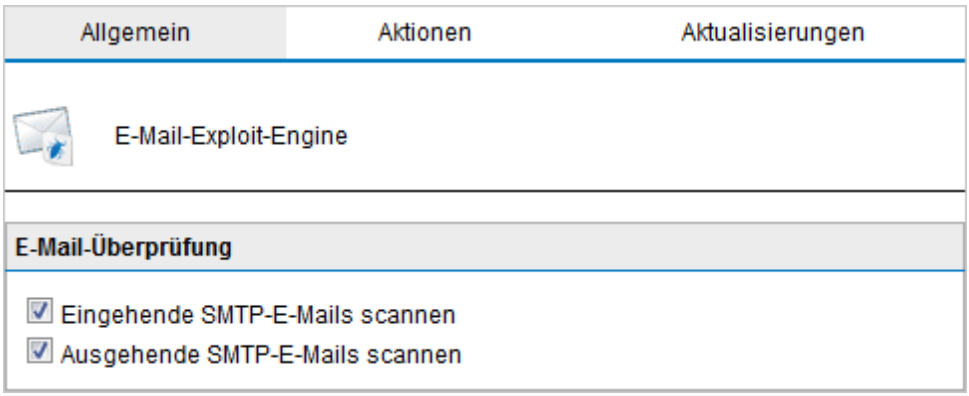
13. Klicken Sie auf **Übernehmen**.

5.4 E-Mail-Exploit-Engine

Die E-Mail-Exploit-Engine blockiert Exploits, die in einer E-Mail eingebettet sind und auf dem Computer des Empfängers ausgeführt werden können, wenn der Benutzer entweder die E-Mail empfängt oder sie öffnet. Ein Exploit nutzt bekannte Schwachstellen in Anwendungen oder Betriebssystemen aus, um die Sicherheit eines Systems zu gefährden. Dabei wird beispielsweise ein Programm oder Befehl ausgeführt oder eine Backdoor installiert.

5.4.1 Konfigurieren der E-Mail-Exploit-Engine

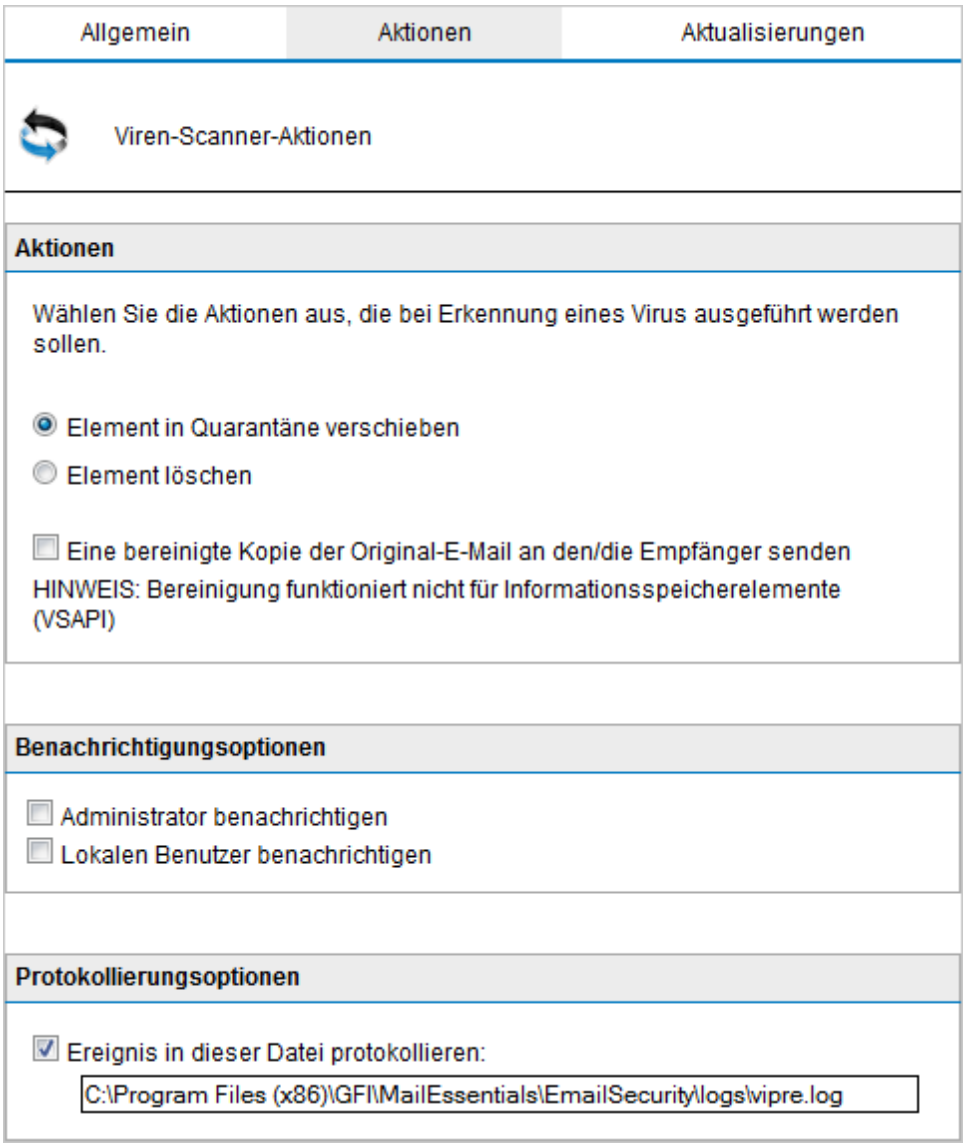
1. Wählen Sie **E-Mail-Sicherheit > E-Mail-Exploit-Engine** aus.



Screenshot 55: Konfiguration der E-Mail-Exploit-Engine

2. Wählen Sie auf der Registerkarte **Allgemein** aus, ob eingehende und/oder ausgehende E-Mails gescannt werden sollen.

Option	Beschreibung
Eingehende SMTP-E-Mails scannen	Wählen Sie diese Option aus, um eingehende E-Mails zu scannen.
Ausgehende SMTP-E-Mails scannen	Wählen Sie diese Option aus, um ausgehende E-Mails zu scannen.



Screenshot 56: Virenscan-Engine: Konfigurationsseite (Registerkarte für Aktionen)

3. Wählen Sie auf der Registerkarte **Aktionen** aus, was geschehen soll, wenn eine E-Mail blockiert wird:

Aktion	Beschreibung
Element in Quarantäne verschieben	Speichert alle infizierten E-Mails, die von der ausgewählten Virenscan-Engine erkannt werden, im Quarantänespeicher. Danach können Sie alle E-Mails in der Quarantäne überprüfen (zulassen/löschen). Weitere Informationen finden Sie unter „Arbeiten mit E-Mails in Quarantäne“ (Seite 217).
Element löschen	Löscht infizierte E-Mails

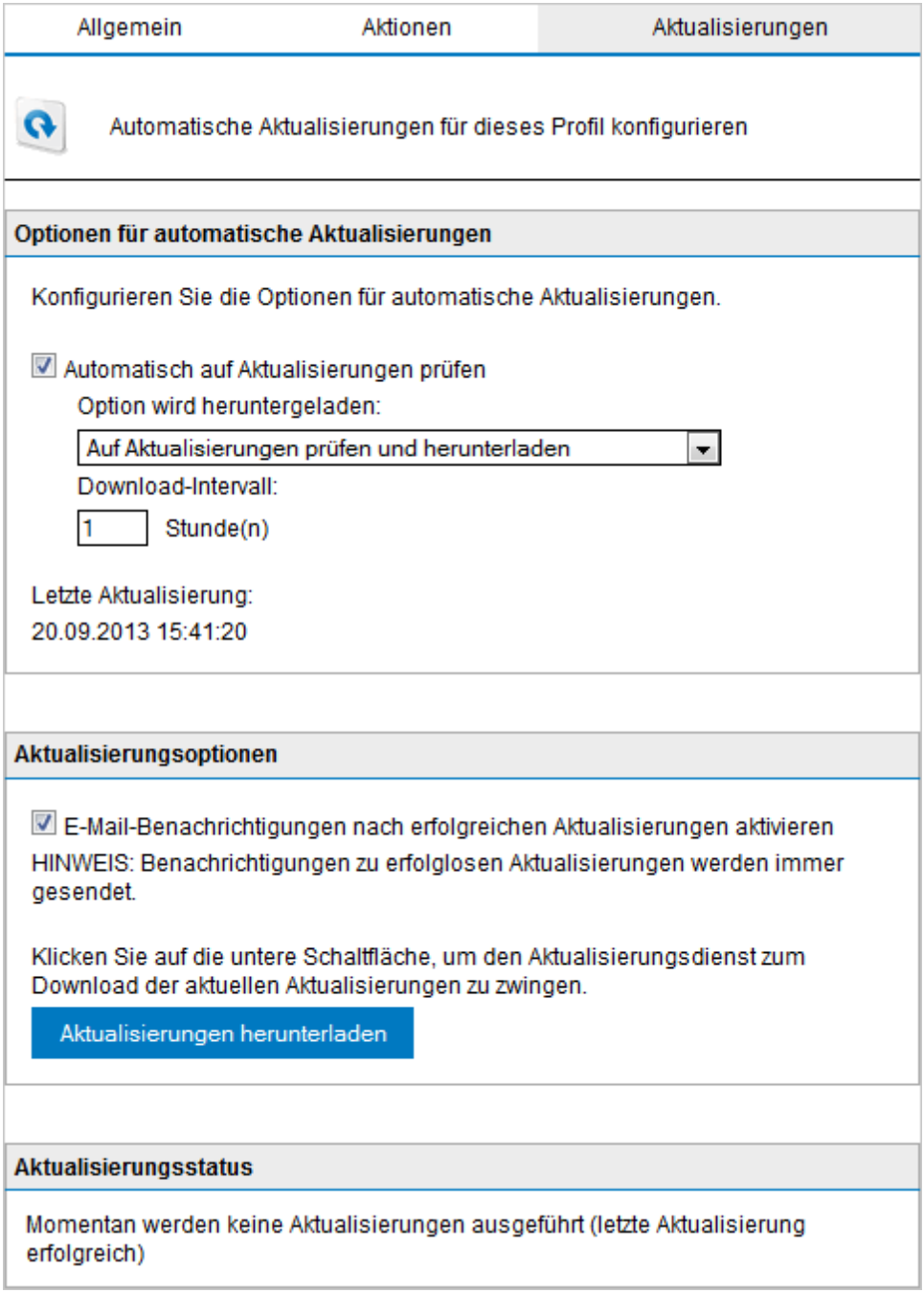
4. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

5. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser**

Datei protokollieren aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log



Screenshot 57: Aktualisierungen für Virenscan-Engines

6. Wählen Sie auf der Registerkarte **Aktualisierungen** die Option **Automatisch auf Aktualisierungen prüfen** aus, um die automatische Aktualisierung der Anti-Virus-Dateien für die ausgewählte Engine zu aktivieren.

7. Wählen Sie in der Liste **Download-Option** eine der folgenden Optionen aus:

Option	Beschreibung
Nur auf Aktualisierungen prüfen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach Aktualisierungen suchen und den Administrator benachrichtigen soll, sobald Aktualisierungen für diese Engine verfügbar sind. Mit dieser Option werden die verfügbaren Aktualisierungen NICHT automatisch heruntergeladen.
Auf Aktualisierungen prüfen und herunterladen	Wählen Sie diese Option aus, wenn GFI MailEssentials nach verfügbaren Aktualisierungen für diese Engine suchen und diese automatisch herunterladen soll.

8. Geben Sie in Form eines Stundenintervalls an, wie oft GFI MailEssentials nach Aktualisierungen für diese Engine suchen bzw. diese herunterladen soll.

9. Wählen Sie im Bereich **Aktualisierungsoptionen** die Option **E-Mail-Benachrichtigungen nach erfolgreichen Aktualisierungen aktivieren**, um eine Benachrichtigung an den Administrator zu senden, wenn die Engine erfolgreich aktualisiert wurde.

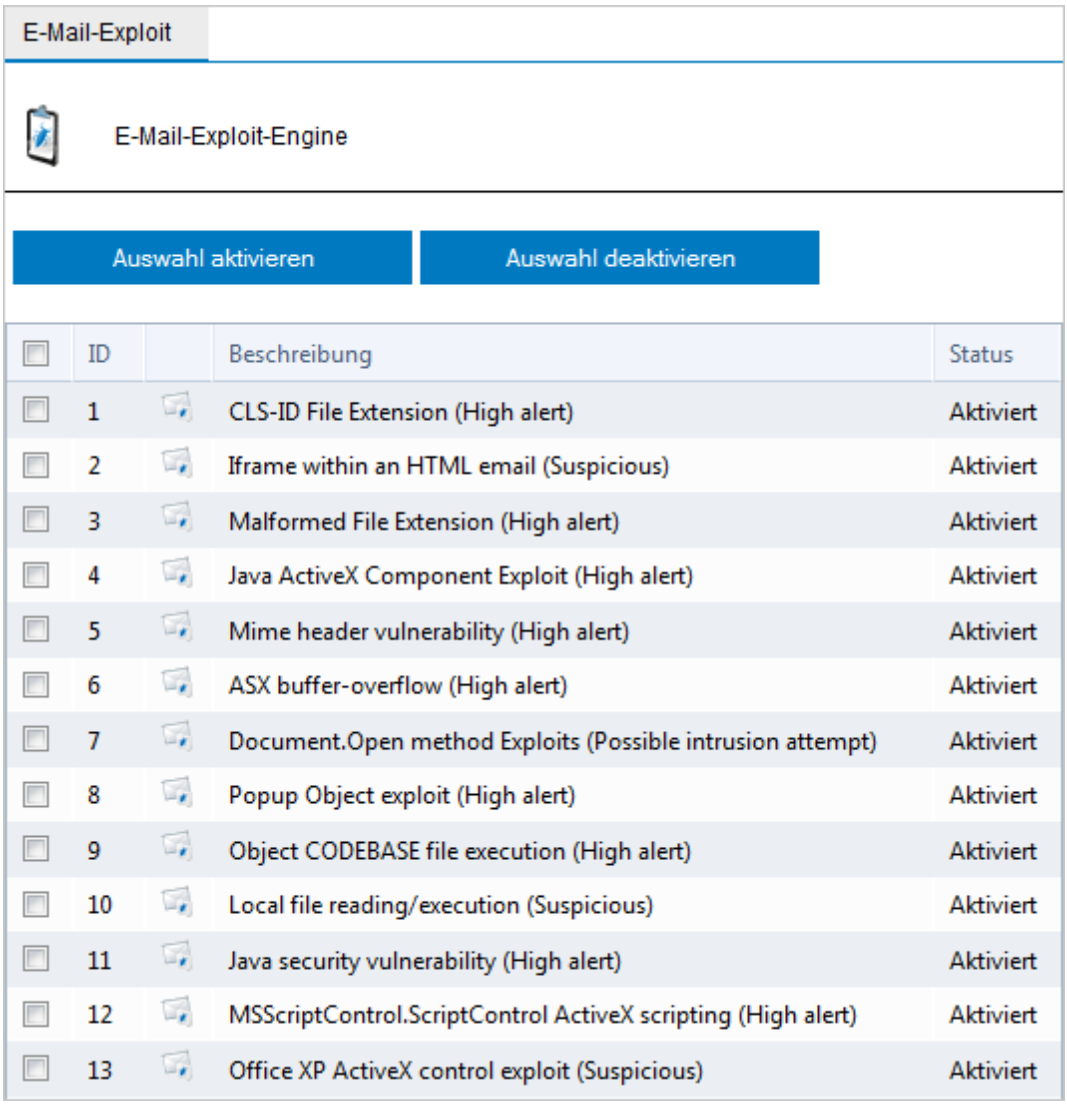
> **HINWEIS**
>
> Wenn Aktualisierungen fehlschlagen, wird immer eine E-Mail-Benachrichtigung gesendet.

10. Klicken Sie auf **Aktualisierungen herunterladen**, um sofort nach Aktualisierungen zu suchen und diese herunterzuladen.

11. Klicken Sie auf **Übernehmen**.

5.4.2 Aktivieren/Deaktivieren von E-Mail-Exploits

1. Wählen Sie **E-Mail-Sicherheit > E-Mail-Exploit-Engine > Exploit-Liste** aus.


E-Mail-Exploit
E-Mail-Exploit-Engine
Auswahl aktivieren
Auswahl deaktivieren
ID
Beschreibung
Status
1 CLS-ID File Extension (High alert) Aktiviert
2 Iframe within an HTML email (Suspicious) Aktiviert
3 Malformed File Extension (High alert) Aktiviert
4 Java ActiveX Component Exploit (High alert) Aktiviert
5 Mime header vulnerability (High alert) Aktiviert
6 ASX buffer-overflow (High alert) Aktiviert
7 Document.Open method Exploits (Possible intrusion attempt) Aktiviert
8 Popup Object exploit (High alert) Aktiviert
9 Object CODEBASE file execution (High alert) Aktiviert
10 Local file reading/execution (Suspicious) Aktiviert
11 Java security vulnerability (High alert) Aktiviert
12 MSScriptControl.ScriptControl ActiveX scripting (High alert) Aktiviert
13 Office XP ActiveX control exploit (Suspicious) Aktiviert

Screenshot 58: Liste der E-Mail-Exploits

2. Markieren Sie die Kontrollkästchen der Exploits, die aktiviert oder deaktiviert werden sollen.

3. Klicken Sie nach Bedarf auf **Auswahl aktivieren** oder **Auswahl deaktivieren**.

5.5 HTML-Bereinigung

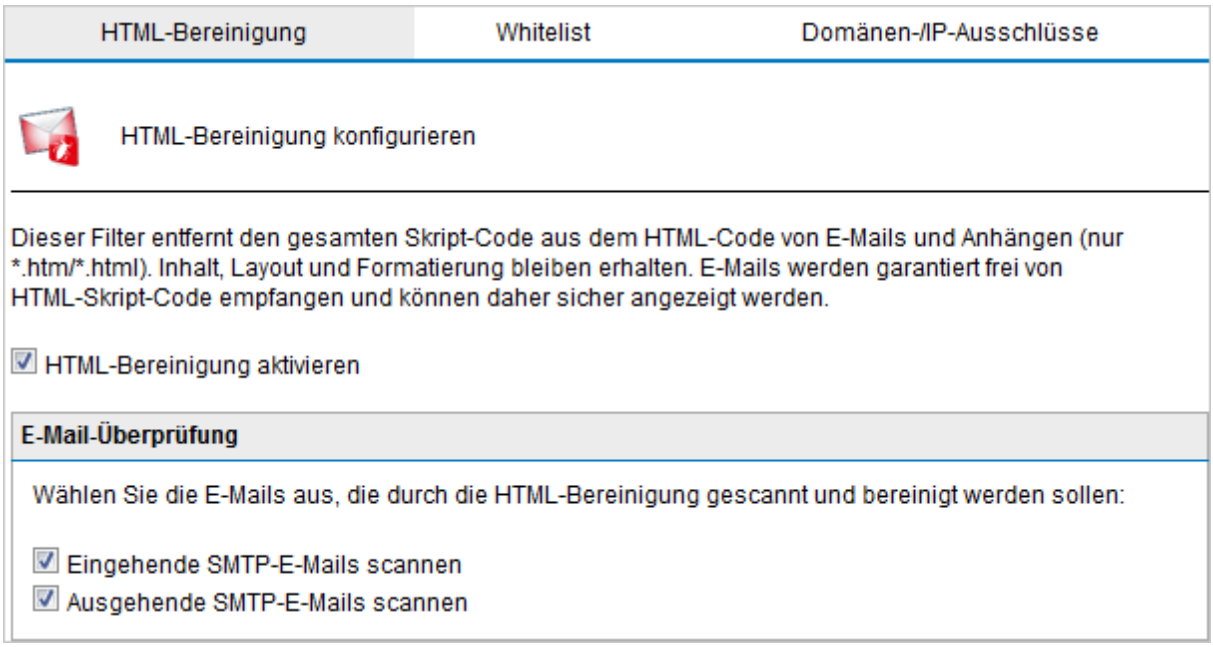
Die HTML-Bereinigung scannt und entfernt Skript-Code im Text oder Anhang von E-Mails. Folgendes wird gescannt:

» Textkörper von E-Mails, deren MIME-Typ auf „text/html“ gesetzt ist

» Alle Anhänge des Typs **.htm** oder **.html**

5.5.1 Konfigurieren der HTML-Bereinigung

1. Wählen Sie **E-Mail-Sicherheit > HTML-Bereinigung** aus.


HTML-Bereinigung
Whitelist
Domänen-/IP-Ausschlüsse
HTML-Bereinigung konfigurieren
Dieser Filter entfernt den gesamten Skript-Code aus dem HTML-Code von E-Mails und Anhängen (nur *.htm/*.html). Inhalt, Layout und Formatierung bleiben erhalten. E-Mails werden garantiert frei von HTML-Skript-Code empfangen und können daher sicher angezeigt werden.
HTML-Bereinigung aktivieren
E-Mail-Überprüfung
Wählen Sie die E-Mails aus, die durch die HTML-Bereinigung gescannt und bereinigt werden sollen:
Eingehende SMTP-E-Mails scannen
Ausgehende SMTP-E-Mails scannen

Screenshot 59: Konfigurationsseite der HTML-Bereinigung

2. Aktivieren Sie die HTML-Bereinigung, indem Sie **HTML-Bereinigung aktivieren** markieren.

3. Wählen Sie die E-Mail-Richtung aus:

Option	Beschreibung
Eingehende SMTP-E-Mails scannen	Die HTML-Skripte aller eingehenden E-Mails werden gescannt und bereinigt.
Ausgehende SMTP-E-Mails scannen	Die HTML-Skripte aller ausgehenden E-Mails werden gescannt und bereinigt.

4. Klicken Sie auf **Übernehmen**.

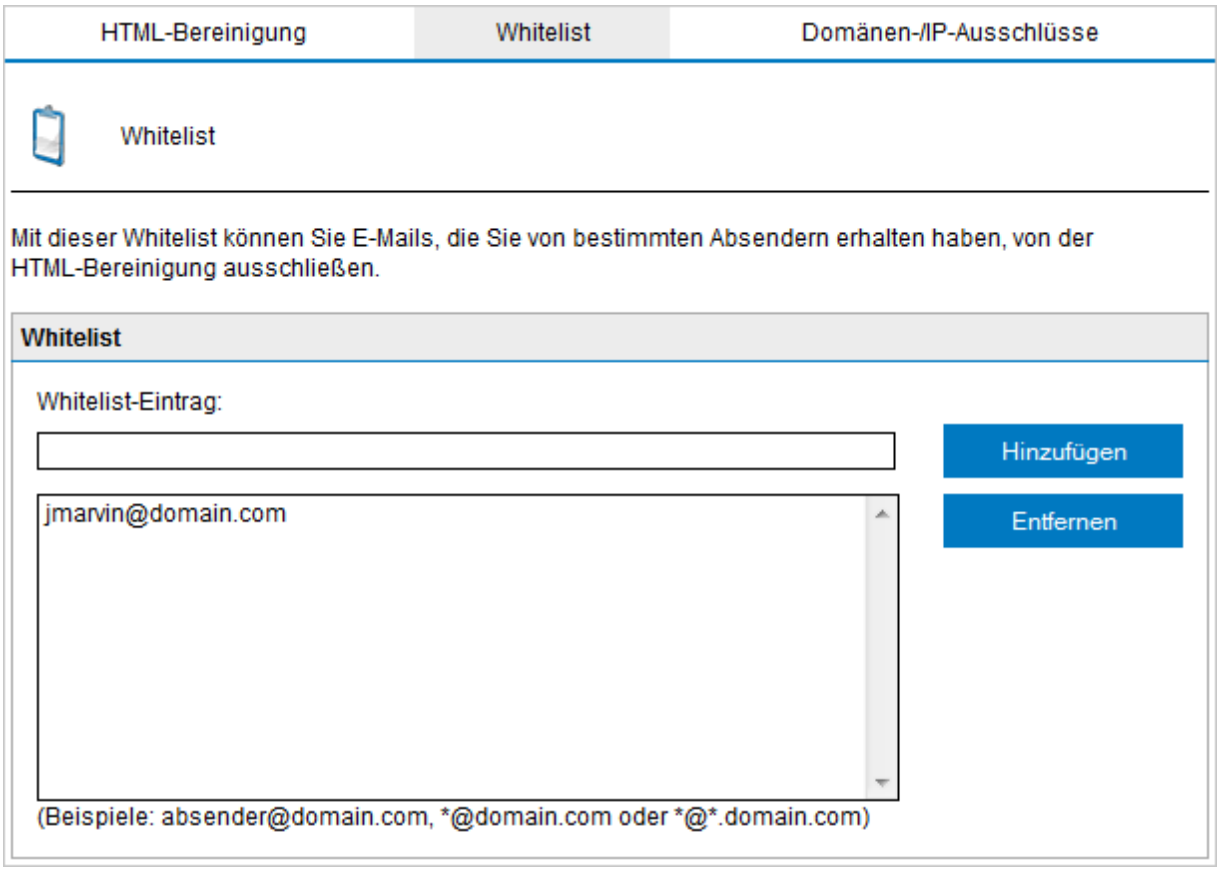
5.5.2 Whitelist der HTML-Bereinigung

Die Whitelist der HTML-Bereinigung kann so konfiguriert werden, dass E-Mails von bestimmten Absendern ausgeschlossen werden.

> **HINWEIS**
>
> Mit der Funktion „Domänen-/IP-Ausschlüsse in der HTML-Bereinigung“ können Sie konkrete IP-Adressen und Domänen ausschließen. Weitere Informationen finden Sie unter „HTML-Bereinigung“ (Seite 107).

So verwalten Sie die Absender in der Whitelist der HTML-Bereinigung:

1. Wählen Sie **E-Mail-Sicherheit > HTML-Bereinigung** und anschließend die Registerkarte **Whitelist** aus.



Screenshot 60: Whitelist-Seite der HTML-Bereinigung

2. Geben Sie unter **Whitelist-Eintrag** eine E-Mail-Adresse, eine E-Mail-Domäne (z. B. *@domain.com) oder eine E-Mail-Subdomäne (z. B. *@*.domain.com) ein, und klicken Sie auf **Hinzufügen**.

> **HINWEIS**
>
> Zum Entfernen eines Eintrags aus der Whitelist der HTML-Bereinigung wählen Sie diesen aus, und klicken Sie auf **Entfernen**.

3. Klicken Sie auf **Übernehmen**.

5.5.3 Domänen-/IP-Ausschlüsse in der HTML-Bereinigung

Mit der Funktion Domänen-/IP-Ausschlüsse in der HTML-Bereinigung können Administratoren konkrete IP-Adressen und Domänen von der HTML-Bereinigung ausschließen. Hier können nicht nur IP-Adresslisten, sondern auch Domänenadressen angegeben werden, die dann zur Laufzeit aufgelöst werden, um alle IP-Adressen für die fragliche Domäne zu erhalten. Hierfür gibt es zwei Möglichkeiten:

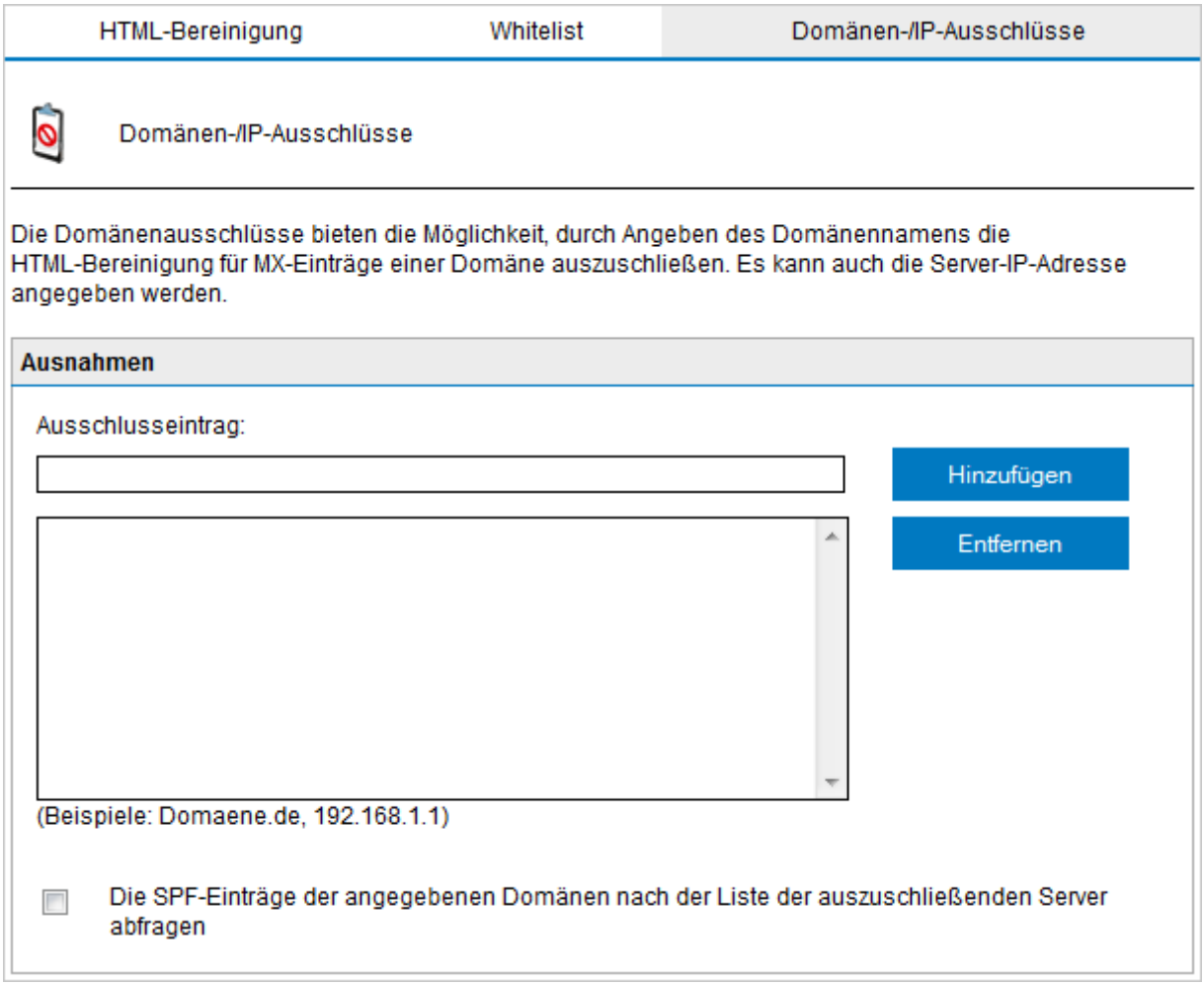
1. Standardmäßig fragt die Funktion den MX-Eintrag der gerade verarbeiteten Domäne ab

2. Optional können Sie den SPF-Eintrag der abgefragten Domäne erhalten. Verfügt die Domäne über keinen SPF-Eintrag, wird der SPF-Teil ignoriert und nur die MX-Einträge verwendet.

Falls die IP-Adresse, von der die E-Mail stammt (die Adresse, die die E-Mail an den Perimeter-Server gesendet hat), in der Registerkarte mit Domänen-/IP-Ausschlüssen aufgeführt ist oder sich als Auflösung einer Domäne auf dieser Liste ergibt, wird sie vom HTML-Bereiniger nicht verarbeitet. Die Liste ähnelt also einer IP-Whitelist, ermöglicht aber zusätzlich die Angabe von Domänen sowie die Auflösung des MX-Eintrags (oder optional des SPF-Eintrags) der Domäne, um die IP-Adresse zu erhalten.

Domänen-/IP-Ausschlüsse in der Whitelist der HTML-Bereinigung verwalten:

1. Wählen Sie **E-Mail-Sicherheit > HTML-Bereinigung** und anschließend die Registerkarte **Domänen-/IP-Ausschlüsse** aus.


HTML-Bereinigung
Whitelist
Domänen-/IP-Ausschlüsse
Domänen-/IP-Ausschlüsse
Die Domänenausschlüsse bieten die Möglichkeit, durch Angeben des Domänennamens die HTML-Bereinigung für MX-Einträge einer Domäne auszuschließen. Es kann auch die Server-IP-Adresse angegeben werden.
Ausnahmen
Ausschlusseintrag:
Hinzufügen
Entfernen
(Beispiele: Domaene.de, 192.168.1.1)
Die SPF-Einträge der angegebenen Domänen nach der Liste der auszuschließenden Server abfragen

Screenshot 61: Domänen-/IP-Ausschlüsse

2. Geben Sie eine auszuschließende Domäne oder IP-Adresse ein, und klicken Sie auf **Hinzufügen**.

> **HINWEIS**
>
> Zum Entfernen eines Eintrags aus den Domänen-/IP-Ausschlüssen in der HTML-Bereinigung wählen Sie diesen aus, und klicken Sie auf **Entfernen**.

3. Optional wählen Sie **Die SPF-Einträge der angegebenen Domänen nach der Liste der auszuschließenden Server abfragen**.

4. Klicken Sie auf **Übernehmen**.

6 Anti-Spam

Die in GFI MailEssentials enthaltenen Anti-Spam-Filter unterstützen das Erkennen und Blockieren unerwünschter E-Mails (Spam).

Themen in diesem Kapitel:

6.1 Anti-Spam-Filter **111**

6.2 Spam-Aktionen – Umgang mit Spam-E-Mails **150**

6.3 Sortieren der Anti-Spam-Filter nach Priorität **153**

6.4 SMTP-Übertragungsfilterung **154**

6.5 Spam-Bericht **156**

6.6 Anti-Spam-Einstellungen **158**

6.7 SpamTag für Microsoft Outlook **166**

6.8 Scannen öffentlicher Ordner **174**

6.1 Anti-Spam-Filter

GFI MailEssentials setzt verschiedene Scan-Filter zur Identifizierung von Spam ein:

FILTER	BESCHREIBUNG	STANDARDMÄSSIG AKTIVIERT
SpamRazer	Eine Anti-Spam-Engine, die anhand der E-Mail-Reputation, des Nachrichtenfingerabdrucks und der Inhaltsanalyse bestimmt, ob eine E-Mail als Spam einzustufen ist.	Ja
Anti-Phishing	Blockiert E-Mails, die typische Phishing-Stichwörter oder Links enthalten, die auf bekannte Phishing-Websites verweisen.	Ja
Directory Harvesting	Directory Harvesting-Angriffe treten auf, wenn Spammer versuchen, E-Mail-Adressen zu erraten, indem sie Ihrer Domäne bekannte Benutzernamen hinzufügen. Die Mehrheit der E-Mail-Adressen existiert nicht.	Ja (nur wenn GFI MailEssentials in einer Active Directory-Umgebung installiert ist)
E-Mail-Blocklist	Die E-Mail-Blocklist ist eine von Ihnen definierte Datenbank mit E-Mail-Adressen und Domänen, von denen Sie auf keinen Fall E-Mails erhalten möchten.	Ja
IP-Blocklist	Die IP-Blocklist ist eine von Ihnen definierte Datenbank mit IP-Adressen, von denen Sie auf keinen Fall E-Mails erhalten möchten.	Nein
IP-DNS-Blocklist	Die IP-DNS-Blocklist vergleicht die IP-Adressen der sendenden Mailserver mit einer öffentlichen Liste von Mailservern, die bekanntermaßen Spam versenden.	Ja
URI-DNS-Blocklist	Stoppt E-Mails, wenn sie Links zu Domänen enthalten, die in öffentlichen Spam-URI-Blocklists aufgeführt sind.	Ja
Sender Policy Framework	Dieser Filter blockiert E-Mails von gefälschten IP-Adressen, indem er mithilfe von SPF-Einträgen prüft, ob die jeweilige Absender-IP-Adresse autorisiert ist.	Nein
Anti-Spoofing	Dieser Filter vergleicht E-Mails, deren Absenderadresse mit Ihrer eigenen Domäne übereinzustimmen scheint, mit einer Liste von IP-Adressen in GFI MailEssentials. Befindet sich die Absender-IP-Adresse nicht in der Liste mit den Server-IP-Adressen der eigenen Domäne, wird die E-Mail blockiert.	Nein
Greylist	Der Greylist-Filter blockiert temporär eingehende E-Mails von unbekannten Absendern. Zulässige Mailsysteme versuchen normalerweise, die E-Mail nach einigen Minuten erneut zu senden, Spammer hingegen ignorieren solche Fehlernachrichten einfach.	Nein

FILTER	BESCHREIBUNG	STANDARDMÄSSIG AKTIVIERT
Header-Prüfung	Der Filter zur Header-Kontrolle analysiert E-Mail-Header, um Spam-Mails zu erkennen.	Ja
Spam-Stichwortprüfung	Dieser Filter ermöglicht die Erkennung von Spam auf der Basis von Stichwörtern in eingehenden E-Mails.	Nein
Bayes'sche Analyse	Ein Anti-Spam-Filter kann so trainiert werden, dass er auf der Basis von Erfahrungswerten genau bestimmen kann, ob es sich bei einer E-Mail um Spam handelt.	Nein
Whitelist	Die Whitelist enthält Listen von Kriterien, die zulässige E-Mails identifizieren. E-Mails, die diesen Kriterien entsprechen, werden nicht von Anti-Spam-Filtern geprüft und immer direkt dem Empfänger zugestellt.	Ja
Neue Absender	Der Filter für neue Absender identifiziert E-Mails von Absendern, an die bislang keine E-Mails gesendet wurden.	Nein

6.1.1 SpamRazer

Eine Anti-Spam-Engine, die anhand der E-Mail-Reputation, des Nachrichtenfingerabdrucks und der Inhaltsanalyse bestimmt, ob eine E-Mail als Spam einzustufen ist. SpamRazer ist die primäre Anti-Spam-Engine. Sie wird bei der Installation standardmäßig aktiviert. Für SpamRazer werden regelmäßig Aktualisierungen veröffentlicht, die die Reaktion auf neue Spam-Trends kontinuierlich verkürzen.

SpamRazer beinhaltet auch eine Sender Policy Framework-Filterung zur Erkennung gefälschter Absender. Es wird empfohlen, dass Absender ihre Mailserver zu diesem Zweck in einem SPF-Eintrag veröffentlichen. Weitere Informationen zu SPF und der genauen Funktionsweise finden Sie auf der Sender Policy Framework-Website: http://www.openspf.org.

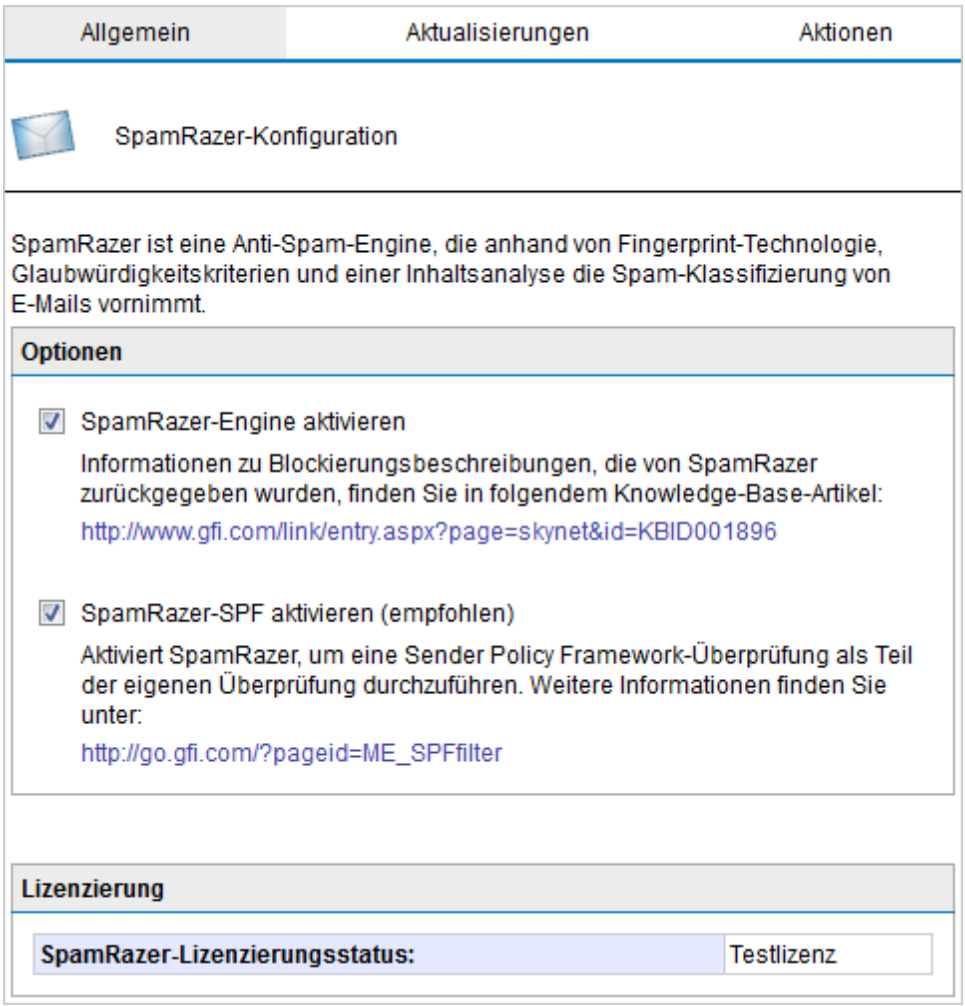
Dieser Filter blockiert auch NDR-Spam (gefälschte Unzustellbarkeitsberichte). Weitere Informationen zu NDR-Spam finden Sie unter http://go.gfi.com/?pageid=ME_NDRSpam.

Konfigurieren von SpamRazer

> **HINWEIS**
>
> Das Deaktivieren von SpamRazer wird **NICHT** empfohlen.

> **HINWEIS**
>
> GFI MailEssentials lädt Aktualisierungen für SpamRazer von folgender Website herunter:
>
> *.mailshell.net

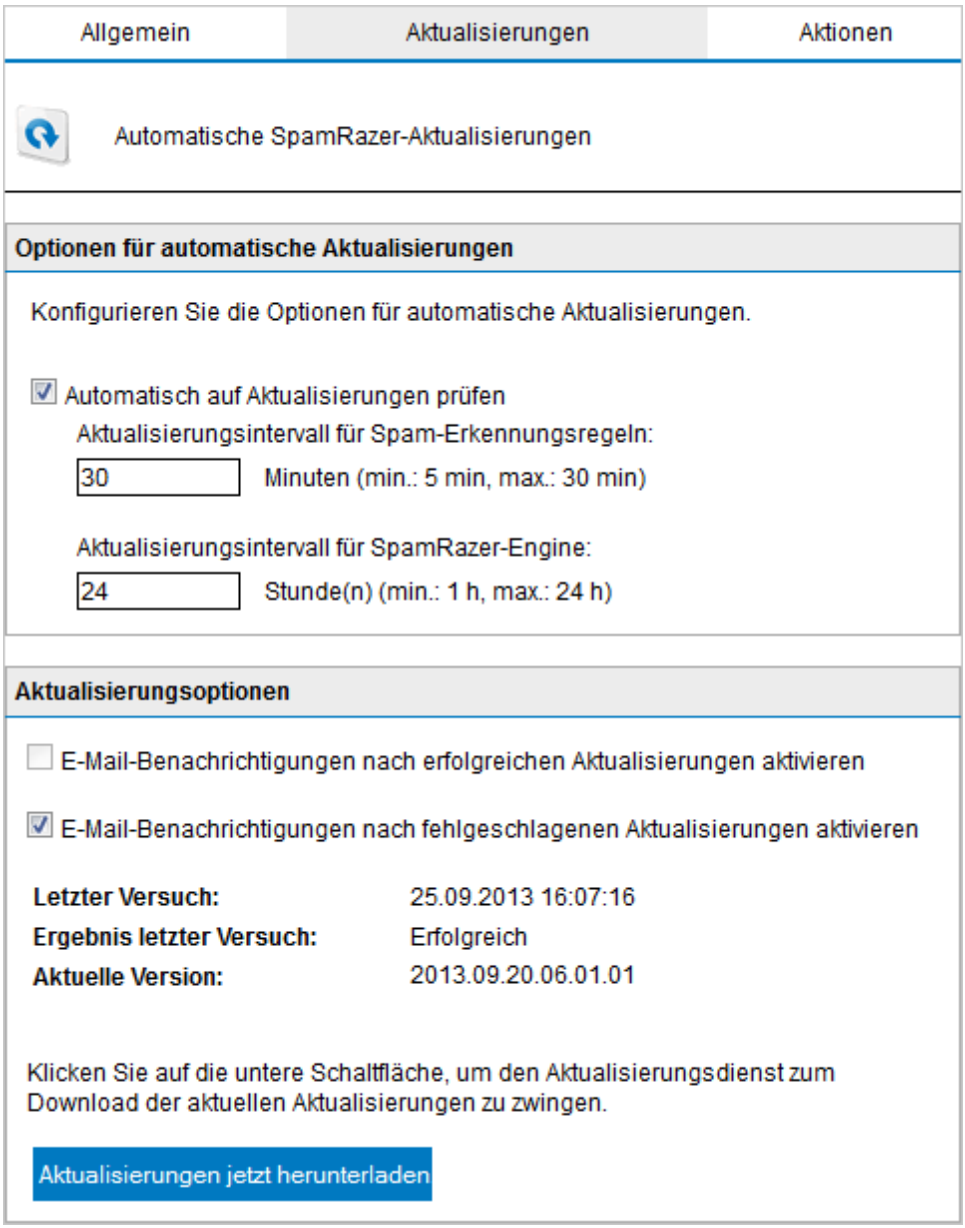
1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > SpamRazer** aus.


Allgemein
Aktualisierungen
Aktionen
SpamRazer-Konfiguration
SpamRazer ist eine Anti-Spam-Engine, die anhand von Fingerprint-Technologie, Glaubwürdigkeitskriterien und einer Inhaltsanalyse die Spam-Klassifizierung von E-Mails vornimmt.
Optionen
SpamRazer-Engine aktivieren
Informationen zu Blockierungsbeschreibungen, die von SpamRazer zurückgegeben wurden, finden Sie in folgendem Knowledge-Base-Artikel:
http://www.gfi.com/link/entry.aspx?page=skynet&id=KBID001896
SpamRazer-SPF aktivieren (empfohlen)
Aktiviert SpamRazer, um eine Sender Policy Framework-Überprüfung als Teil der eigenen Überprüfung durchzuführen. Weitere Informationen finden Sie unter:
http://go.gfi.com/?pageid=ME_SPFfilter
Lizenzierung
SpamRazer-Lizenzierungsstatus:
Testlizenz

Screenshot 62: Eigenschaften von SpamRazer

2. Auf der Registerkarte **Allgemein** können Sie Folgendes tun:

Option	Beschreibung
SpamRazer-Engine aktivieren	SpamRazer aktivieren oder deaktivieren.
SpamRazer-SPF aktivieren (empfohlen)	Sender Policy Framework aktivieren oder deaktivieren. Es wird empfohlen, diese Option zu aktivieren und den Filter nach der Whitelist-Prüfung für E-Mails auszuführen.



Screenshot 63: Registerkarte für SpamRazer-Aktualisierungen

3. Auf der Registerkarte **Aktualisierungen** können Sie Folgendes tun:

Option	Beschreibung
Automatisch auf Aktualisierungen prüfen	Sie können GFI MailEssentials so konfigurieren, dass automatisch nach SpamRazer-Aktualisierungen gesucht wird und diese heruntergeladen werden. Sie können angeben, in welchem Zeitintervall (in Minuten) nach Aktualisierungen für Spam-Erkennungsregeln und für die SpamRazer-Engine gesucht werden soll. **HINWEIS** Es wird empfohlen, diese Option für SpamRazer zu aktivieren, damit die neuesten Spam-Trends effektiv erkannt werden.
E-Mail-Benachrichtigungen nach erfolgreichen Aktualisierungen aktivieren	Wählen Sie diese Option aus, wenn Sie per E-Mail informiert werden möchten, sobald neue Aktualisierungen heruntergeladen werden.

Option	Beschreibung
E-Mail-Benachrichtigungen nach fehlgeschlagenen Aktualisierungen aktivieren	Wählen Sie diese Option aus, wenn Sie per E-Mail informiert werden möchten, falls ein Download oder eine Installation fehlschlägt.
Aktualisierungen jetzt herunterladen ...	Klicken Sie hier, um Updates herunterzuladen.

> **HINWEIS**
>
> Sie können Aktualisierungen über einen Proxy-Server herunterladen. Weitere Informationen finden Sie unter „Proxy-Einstellungen“ (Seite 246).

4. Klicken Sie auf die Registerkarte **Aktionen**, um auszuwählen, was mit Nachrichten geschehen soll, die als Spam identifiziert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

5. Klicken Sie auf **Übernehmen**.

6.1.2 Anti-Phishing

Blockiert E-Mails, die typische Phishing-Stichwörter oder Links enthalten, die auf bekannte Phishing-Websites verweisen. Phishing ist eine E-Mail-basierte Technik zur sozialen Manipulation, die darauf abzielt, dass E-Mail-Benutzer den Spammern persönliche Daten zur Verfügung stellen. Phishing-E-Mails sind meist wie offizielle Anschreiben gestaltet, beispielsweise wie eine Bankmitteilung. Normalerweise enthalten Phishing-E-Mails Anweisungen, die den Benutzer zur Rückbestätigung sensibler Informationen wie Online-Banking-Daten oder Kreditkartendaten auffordern. Zu diesem Zweck wird in der Phishing-E-Mail ein Uniform Resource Identifier (URI) bzw. Link angegeben, über den der Benutzer auf eine Website geleitet wird, auf der er seine Daten eingeben soll. Diese Site sieht wie der offizielle Webauftritt des vorgetäuschten Absenders aus, wurde aber vom Absender der Phishing-E-Mail nur zum Abschöpfen der Daten eingerichtet. Gibt ein Anwender nun seine vertraulichen Daten auf der Phishing-Site ein, gehen diese direkt an den Angreifer und können von ihm missbraucht werden.

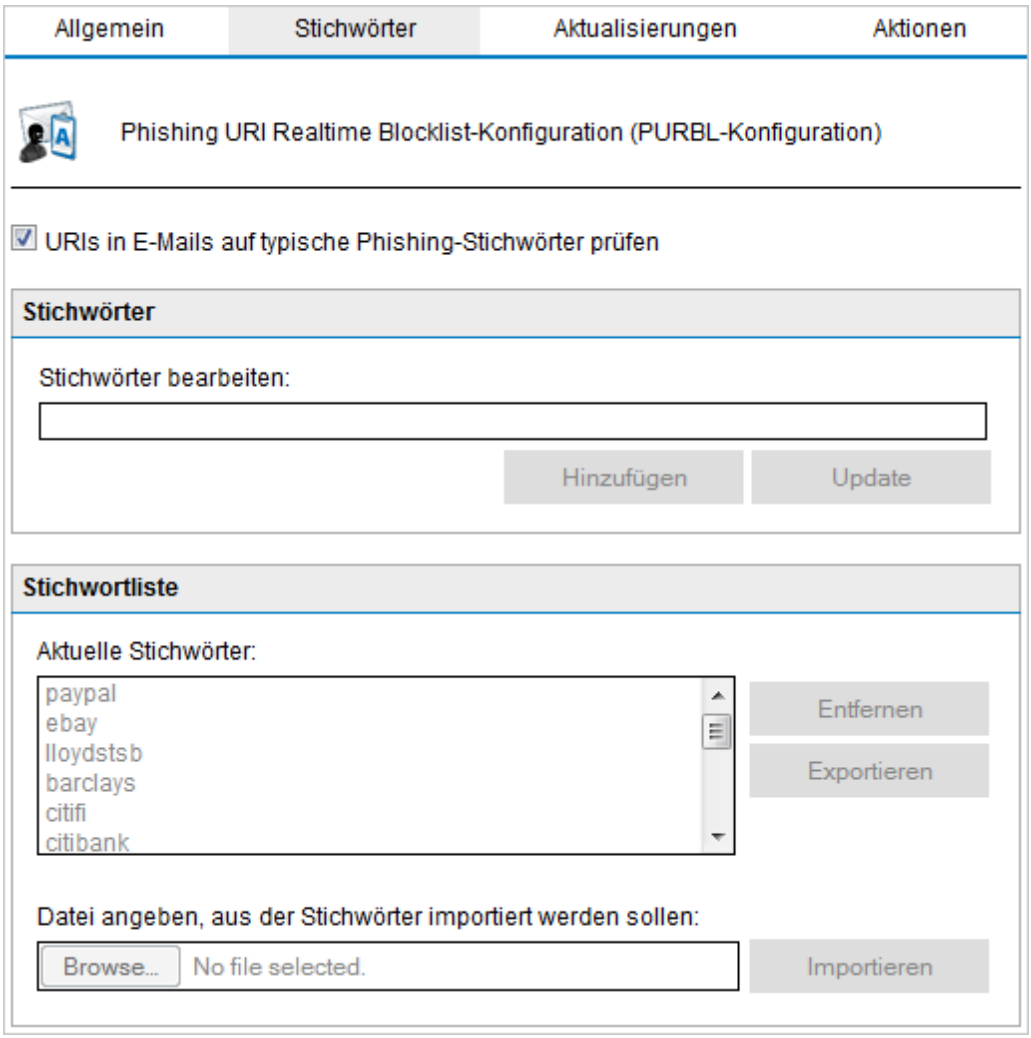
Der Anti-Phishing-Filter erkennt Phishing-Nachrichten, indem er die in einer E-Mail enthaltenen URIs mit einer Datenbank mit bereits bekannten Phishing-URIs vergleicht. Zusätzlich wird in den URIs nach typischen Phishing-Stichwörtern gesucht.

Der Anti-Phishing-Filter wird bei der Installation standardmäßig aktiviert.

Konfigurieren von Anti-Phishing

> **HINWEIS**
>
> Das Deaktivieren von Anti-Phishing wird **NICHT** empfohlen.

1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > Anti-Phishing** aus.



Screenshot 64: Optionen für Anti-Phishing

2. Aktivieren/deaktivieren Sie auf der Registerkarte **Allgemein** die Option **E-Mails auf URIs bekannter Phishing-Websites prüfen**, um Anti-Phishing zu aktivieren/deaktivieren.

3. Wählen Sie auf der Registerkarte **Stichwörter** nach Bedarf die folgenden Optionen aus:

Option	Beschreibung
URIs in E-Mails auf typische Phishing-Stichwörter prüfen	Prüfung auf typische Phishing-Stichwörter aktivieren/deaktivieren
Hinzufügen	Ermöglicht das Hinzufügen von Stichwörtern zum Phishing-Filter. Geben Sie ein Stichwort ein, und klicken Sie auf **Hinzufügen**, um das Stichwort dem Anti-Phishing-Filter hinzuzufügen.
Update	Ermöglicht die Aktualisierung ausgewählter Stichwörter. Wählen Sie in der Liste **Aktuelle Stichwörter** ein Stichwort aus, ändern Sie es im Feld **Stichwörter bearbeiten** nach Bedarf, und klicken Sie auf **Aktualisieren**.
Entfernen	Ermöglicht das Entfernen ausgewählter Stichwörter aus der Liste. Wählen Sie in der Liste **Aktuelle Stichwörter** ein Stichwort aus, und klicken Sie auf **Entfernen**.
Exportieren	Exportiert die aktuelle Liste in eine XML-Datei.
Durchsuchen ...	Ermöglicht das Importieren einer zuvor exportieren Stichwortliste. Klicken Sie auf **Durchsuchen**, wählen Sie eine zuvor exportierte Stichwortdatei aus, und klicken Sie auf **Importieren**.

4. Wählen Sie auf der Registerkarte **Aktualisierungen** nach Bedarf die folgenden Optionen aus:

Option	Beschreibung
Automatisch auf Aktualisierungen prüfen	Konfigurieren Sie GFI MailEssentials so, dass automatisch nach Anti-Phishing-Aktualisierungen gesucht und diese heruntergeladen werden. Geben Sie an, in welchem Zeitintervall (in Minuten) nach Aktualisierungen gesucht werden soll. **HINWEIS** Es wird empfohlen, diese Option für das Anti-Phishing zu aktivieren, damit die neuesten Phishing-Trends effektiv erkannt werden.
E-Mail-Benachrichtigungen nach erfolgreichen Aktualisierungen aktivieren	Wählen Sie aus, ob Sie per E-Mail informiert werden möchten, wenn neue Aktualisierungen heruntergeladen werden.
E-Mail-Benachrichtigungen nach fehlgeschlagenen Aktualisierungen aktivieren	Wählen Sie aus, ob Sie informiert werden möchten, wenn ein Download oder eine Installation fehlschlägt.
Aktualisierungen jetzt herunterladen...	Klicken Sie hier, um Anti-Phishing-Aktualisierungen jetzt herunterzuladen.

HINWEIS

Sie können Aktualisierungen über einen Proxy-Server herunterladen. Weitere Informationen finden Sie unter „Proxy-Einstellungen“ (Seite 246).

5. Klicken Sie auf die Registerkarte **Aktionen**, um auszuwählen, was mit Nachrichten geschehen soll, die als Spam identifiziert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

6. Klicken Sie auf **Übernehmen**.

6.1.3 Directory Harvesting

Directory Harvesting-Angriffe treten auf, wenn Spammer versuchen, E-Mail-Adressen zu erraten, indem sie Ihrer Domäne bekannte Benutzernamen hinzufügen. Die Mehrheit der E-Mail-Adressen existiert nicht.Spammer senden E-Mails an zufällig generierte E-Mail-Adressen. Dabei entsprechen vielleicht manche Adressen echten Benutzern, aber die Mehrheit der Nachrichten ist ungültig und überflutet folglich den Mailserver des Opfers.

GFI MailEssentials wehrt diese Art von Angriffen ab, indem E-Mails mit Empfängern, die auf dem Mailserver oder im Active Directory des Unternehmens nicht existieren, blockiert werden.

Der Directory Harvesting-Filter kann so konfiguriert werden, dass er entweder beim Empfang der vollständigen E-Mail ausgeführt wird, oder dass er eingehende E-Mails auf SMTP-Ebene filtert. Bei der Filterung auf SMTP-Ebene wird die Verbindung zur E-Mail getrennt und somit das Herunterladen der vollständigen E-Mail gestoppt. Dies spart Bandbreite und Verarbeitungsressourcen. Die Verbindung wird in diesem Fall sofort getrennt, und die E-Mail muss keine weiteren Anti-Spam-Filter durchlaufen.

Dieser Filter wird bei der Installation von GFI MailEssentials in einer Active Directory-Umgebung standardmäßig aktiviert.

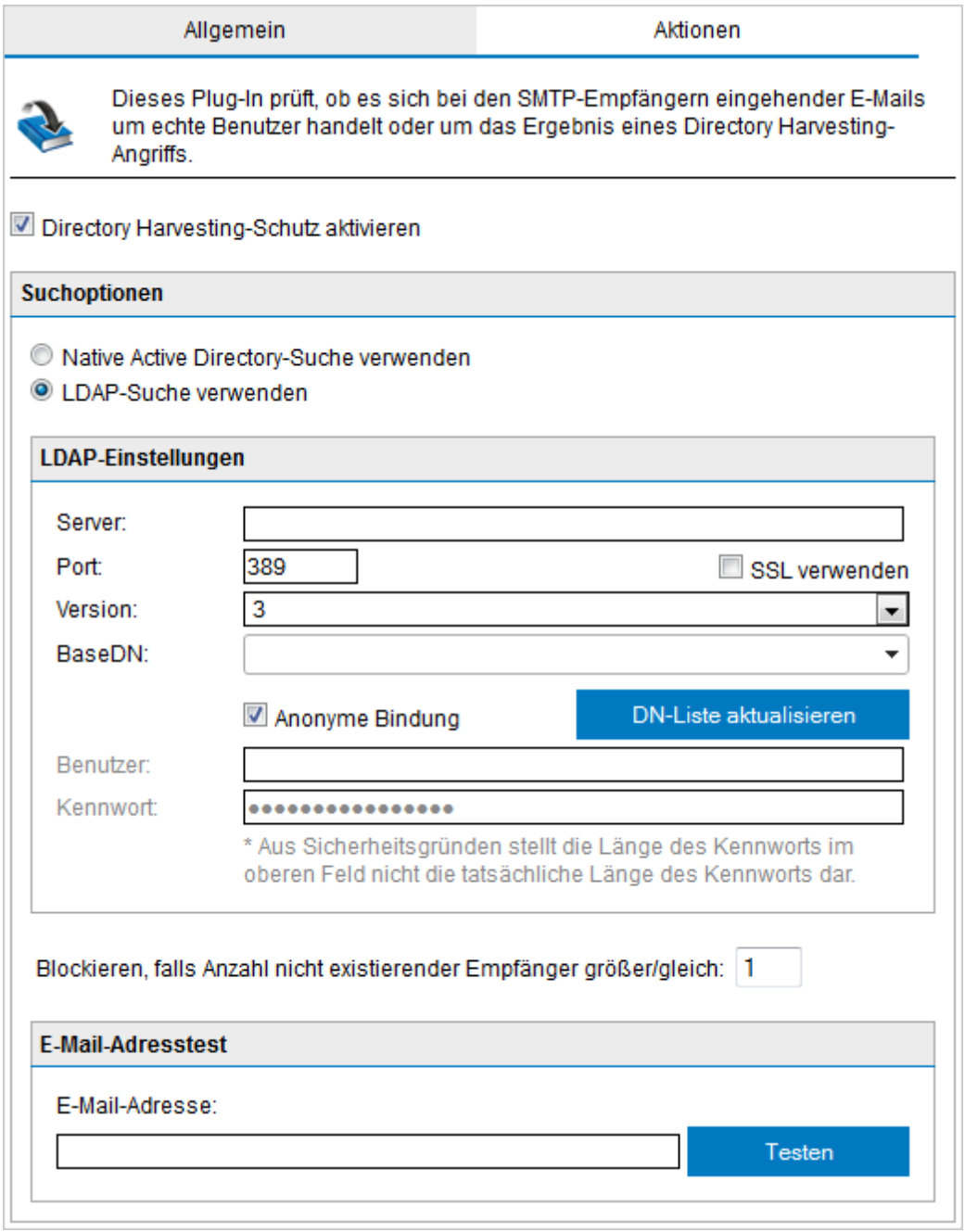
Der Directory Harvesting-Filter wird wie folgt in zwei Phasen eingerichtet.

Phase 1 – Konfigurieren der Directory Harvesting-Eigenschaften

Phase 2 – Auswählen, ob Directory Harvesting während der SMTP-Übertragung ausgeführt werden soll

Phase 1 – Konfigurieren der Directory Harvesting-Eigenschaften

1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > Directory Harvesting** aus.



Screenshot 65: Directory Harvesting-Seite

2. Aktivieren/Deaktivieren Sie Directory Harvesting, und wählen Sie die gewünschte Suchmethode aus:

Option	Beschreibung
Directory Harvesting-Schutz aktivieren	Aktivieren/deaktivieren Sie Directory Harvesting.

Option	Beschreibung
Native Active Directory-Suche verwenden	Wählen Sie diese Option aus, wenn GFI MailEssentials in Active Directory installiert ist. **HINWEIS** Wird GFI MailEssentials hinter einer Firewall betrieben, kann die Directory Harvesting-Funktion möglicherweise aufgrund der Firewall-Einstellungen keine direkte Verbindung mit dem internen Active Directory herstellen. Verwenden Sie für die Verbindung mit dem internen Active Directory Ihres Netzwerks die LDAP-Suche, und stellen Sie sicher, dass der Standardport 389/636 in Ihrer Firewall aktiviert ist.
LDAP-Suche verwenden	Wählen Sie diese Option aus, um Ihre LDAP-Einstellungen zu konfigurieren, wenn GFI MailEssentials im SMTP-Modus installiert ist. Erfordert Ihr LDAP-Server eine Authentifizierung, deaktivieren Sie die Option **Anonyme Bindung**, und geben Sie die Zugangsdaten für diese Funktion ein. **HINWEIS** Geben Sie die Authentifizierungsinformationen im Format Domäne\Benutzer ein (zum Beispiel Hauptdomäne\Administrator). **HINWEIS** In einer Active Directory-Umgebung ist der LDAP-Server üblicherweise der Domänencontroller.

3. Geben Sie unter **Blockieren, falls Anzahl nicht existierender Empfänger größer/gleich** die Anzahl der nicht existierenden Empfänger ein, ab der eine E-Mail als Spam definiert werden soll. E-Mails werden durch Directory Harvesting blockiert, falls alle Empfänger einer E-Mail ungültig sind, oder wenn die Anzahl der ungültigen Empfänger die festgelegte Anzahl übersteigt.

> **HINWEIS**
>
> Vermeiden Sie falsch-positive Ergebnisse, indem Sie eine angemessene Anzahl im Feld **Blockieren, falls Anzahl nicht existierender Empfänger größer/gleich** eingeben. Dieser Wert sollte auch zulässige E-Mails mit falsch geschriebener E-Mail-Adresse sowie E-Mails an Benutzer, die nicht mehr für das Unternehmen arbeiten, berücksichtigen. Es wird empfohlen, dass der Wert mindestens **2** beträgt.

4. Geben Sie eine E-Mail-Adresse ein, und klicken Sie auf **Testen**, um die Einstellungen für Directory Harvesting zu überprüfen. Wiederholen Sie den Test mit einer nicht existierenden E-Mail-Adresse, um sicherzustellen, dass die Suche im Active Directory fehlschlägt.

5. Klicken Sie auf die Registerkarte **Aktionen**, um auszuwählen, was mit Nachrichten geschehen soll, die als Spam identifiziert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

> **HINWEIS**
>
> Wenn Directory Harvesting für die Ausführung auf SMTP-Ebene konfiguriert wurde, ist auf der Registerkarte **Aktionen** nur die Option **Regelereignis in dieser Datei protokollieren** verfügbar.

6. Klicken Sie auf **Übernehmen**.

Phase 2 – Auswählen, ob Directory Harvesting während der SMTP-Übertragung ausgeführt werden soll

1. Wählen Sie **Anti-Spam > Filterpriorität** und anschließend die Registerkarte **SMTP-Übertragungsfilterung** aus.

2. Klicken Sie auf **Wechseln**, um das Directory Harvesting zwischen folgenden beiden Optionen umzuschalten:

Option	Beschreibung
Filtern eingehender vollständiger E-Mails	Die Filterung erfolgt nach dem Empfang der vollständigen E-Mail.
Filtern während der SMTP-Übertragung	Die Filterung erfolgt während der SMTP-Übertragung. Dabei wird vor dem Empfang des E-Mail-Texts und der Anhänge geprüft, ob der E-Mail-Empfänger existiert. **HINWEIS** Bei Auswahl dieser Option wird Directory Harvesting immer vor allen anderen Spam-Filtern ausgeführt.

3. Klicken Sie auf **Übernehmen**.

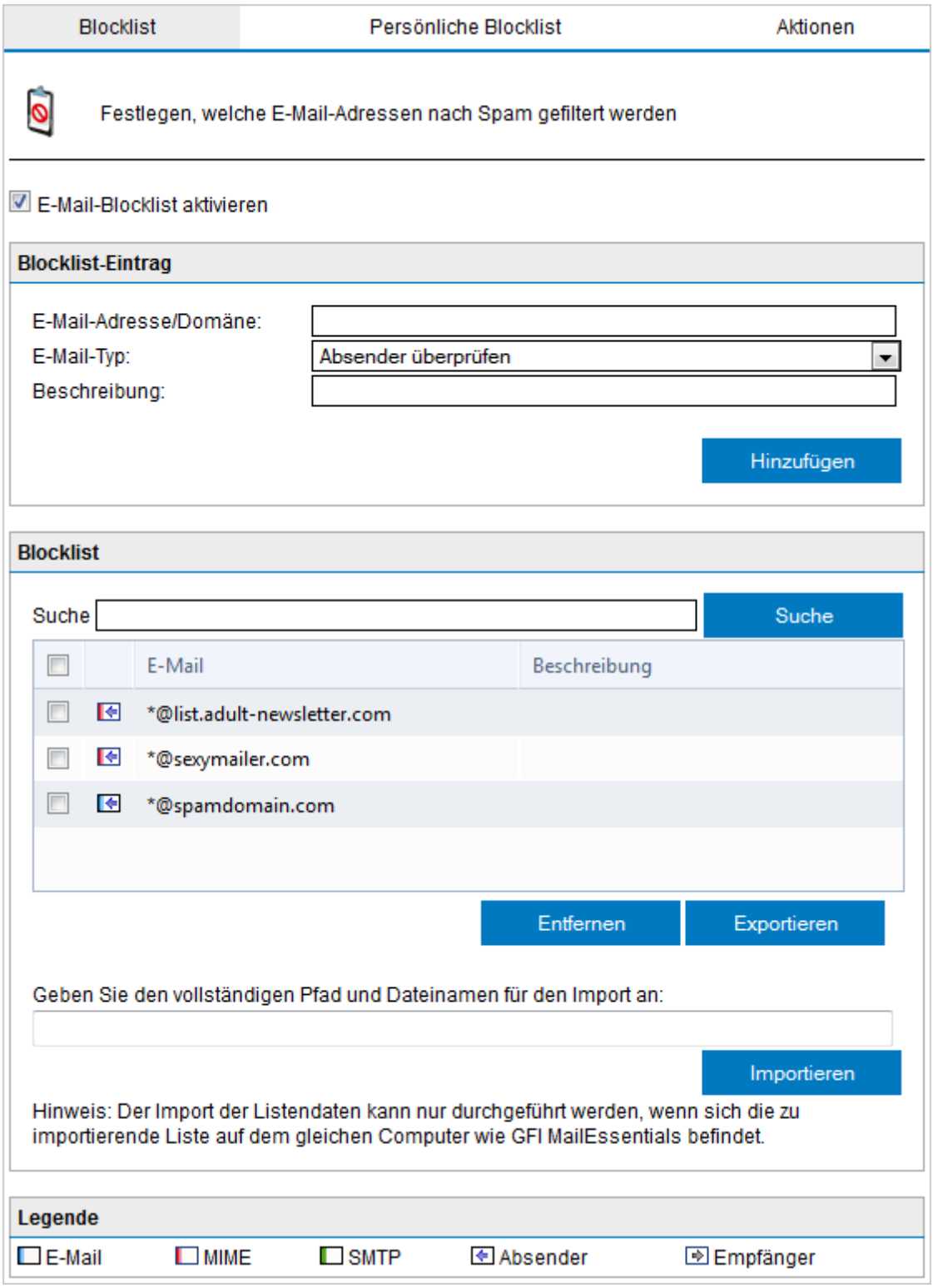
6.1.4 E-Mail-Blocklist

Die E-Mail-Blocklist ist eine von Ihnen definierte Datenbank mit E-Mail-Adressen und Domänen, von denen Sie auf keinen Fall E-Mails erhalten möchten.

Dieser Filter wird bei der Installation von GFI MailEssentials standardmäßig aktiviert.

Konfigurieren der E-Mail-Blocklist

1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > E-Mail-Blocklist** aus.



Screenshot 66: E-Mail-Blocklist

2. Konfigurieren Sie auf der Registerkarte **Blocklist** die E-Mail-Adressen und Domänen, die blockiert werden sollen.

OPTION	BESCHREIBUNG
Aktivieren der E-Mail-Blocklist	Aktivieren/deaktivieren Sie die E-Mail-Blocklist.

OPTION	BESCHREIBUNG
Hinzufügen	Fügen Sie E-Mail-Adressen, E-Mail-Domänen oder Top-Level-Domänen zur Blocklist hinzu. 1. Geben Sie die E-Mail-Adresse, Domäne (z. B. *@spammer.com) oder Top-Level-Domäne (z. B. *@*.tv) ein, die der Blocklist hinzugefügt werden soll. 2. Geben Sie einen E-Mail-Typ an, um entsprechende E-Mails der Blocklist hinzuzufügen. **HINWEIS** Weitere Informationen zum Unterschied zwischen SMTP und MIME finden Sie unter: http://go.gfi.com/?pageid=ME_DifferenceSMTPMIME 3. (Optional) Sie können dem Eintrag im Beschreibungsfeld eine Beschreibung hinzufügen. 4. Klicken Sie auf **Hinzufügen**.
Entfernen	Wählen Sie einen Blocklist-Eintrag aus, und klicken Sie auf **Entfernen**, um ihn zu löschen.
Importieren	Importieren Sie eine Liste von Blocklist-Einträgen aus einer XML-Datei. **HINWEIS** Eine Liste mit Einträgen kann aus einer XML-Datei importiert werden, die dieselbe Struktur wie Exporte von Listeneinträgen aus GFI MailEssentials aufweist.
Exportieren	Exportieren Sie die Liste der Blocklist-Einträge in eine XML-Datei.
Suche	Geben Sie einen Eintrag ein, nach dem gesucht werden soll. Übereinstimmende Einträge werden aus den Blocklist-Einträgen herausgefiltert.

3. Klicken Sie auf die Registerkarte **Aktionen**, um auszuwählen, was mit Nachrichten geschehen soll, die als Spam identifiziert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

4. Klicken Sie auf **Übernehmen**.

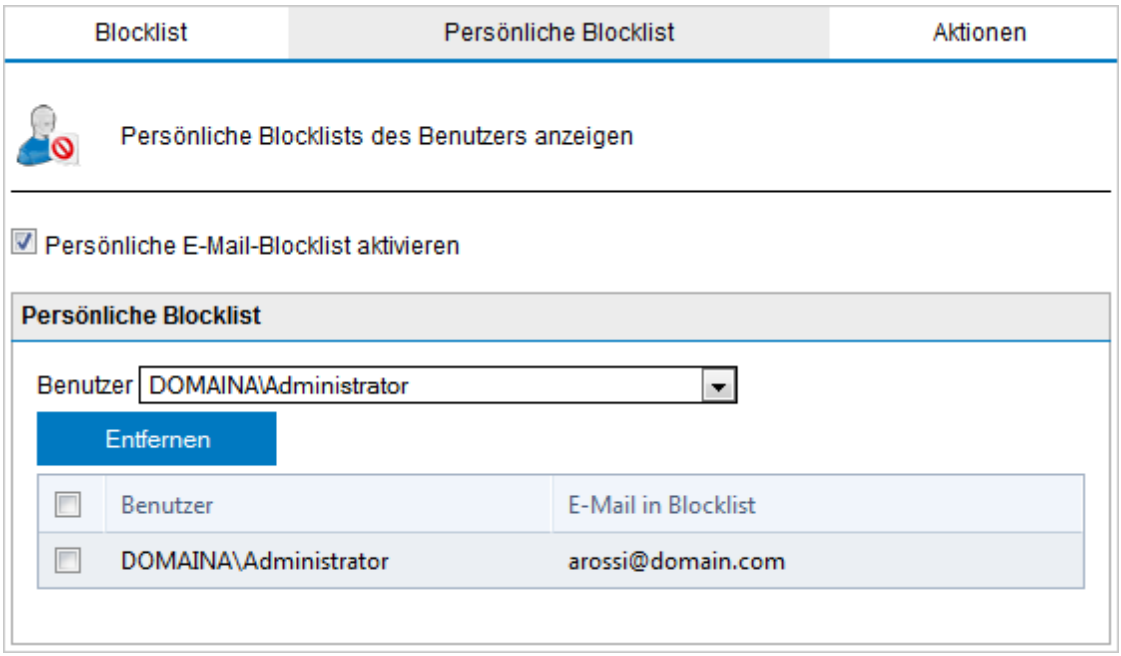
Persönliche Blocklist

Die persönliche Blocklist ist eine zusätzliche Blocklist als Ergänzung zur globalen Blocklist. Sie ist standardmäßig deaktivert und kann zur Aktivierung durch die Benutzer freigeschaltet werden, die dann einer persönlichen, von ihnen verwalteten Blockliste spezifische E-Mail-Adressen hinzufügen können. Weitere Informationen finden Sie unter „Endbenutzeraktionen“ (Seite 19).

Zu Verwaltungszwecken kann der Administrator auch spezifische E-Mail-Adressen entfernen, die die Benutzer zur persönlichen Blocklist hinzugefügt haben.

Aktivieren/Deaktivieren der persönlichen Blocklist

1. Wählen Sie **Anti-Spam > E-Mail-Blocklist** aus.



Screenshot 67: Persönliche Blocklist

2. Wählen Sie die Registerkarte **Persönliche Blocklist** aus und aktivieren oder deaktivieren Sie die Option **Persönliche E-Mail-Blocklist aktivieren**, um die persönliche Blocklist freizuschalten bzw. zu sperren.

3. Klicken Sie auf **Übernehmen**.

Entfernen von E-Mails der persönlichen Blocklist

1. Wählen Sie **Anti-Spam > E-Mail-Blocklist** aus und zeigen Sie dann die Registerkarte **Persönliche Blocklist** an.

2. Wählen Sie aus dem Listenfeld **Benutzer** dann den Benutzer aus, für den eine E-Mail-Adresse gelöscht werden soll.

3. Wählen Sie von der Adressliste eine E-Mail-Adresse aus. Klicken Sie auf **Entfernen**.

4. Klicken Sie auf **Übernehmen**.

6.1.5 IP-Blocklist

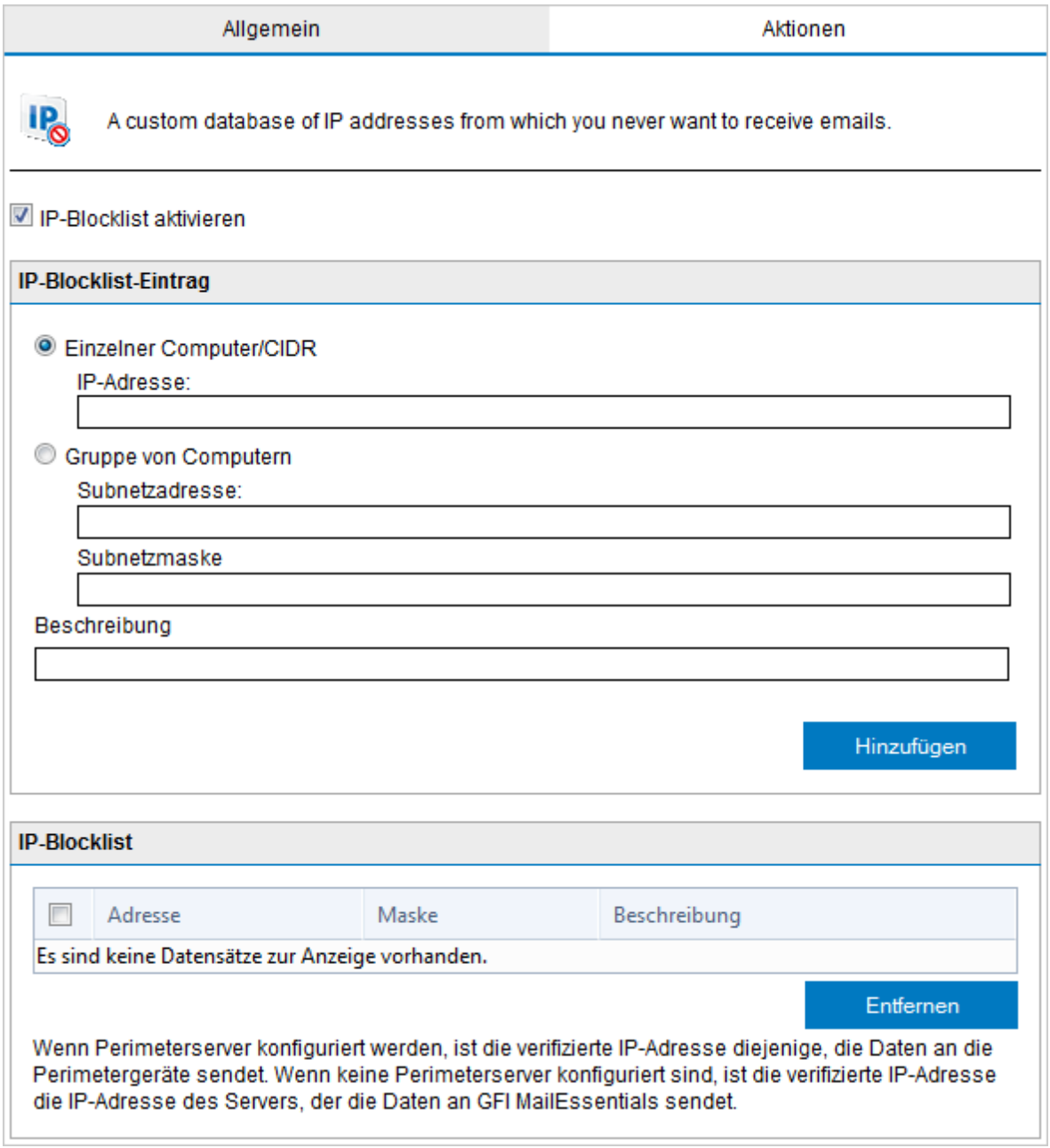
Die IP-Blocklist ist eine von Ihnen definierte Datenbank mit IP-Adressen, von denen Sie auf keinen Fall E-Mails erhalten möchten.

Dieser Filter kann so konfiguriert werden, dass er entweder beim Empfang der vollständigen E-Mail ausgeführt wird, oder dass er eingehende E-Mails auf SMTP-Ebene filtert. Bei der Filterung auf SMTP-Ebene wird die Verbindung zur E-Mail getrennt und somit das Herunterladen der vollständigen E-Mail gestoppt. Dies spart Bandbreite und Verarbeitungsressourcen. Die Verbindung wird in diesem Fall sofort getrennt, und die E-Mail muss keine weiteren Anti-Spam-Filter durchlaufen. Weitere Informationen finden Sie unter „SMTP-Übertragungsfilterung“ (Seite 154).

Die IP-Blocklist ist NICHT standardmäßig aktiviert.

Konfigurieren der Whitelist

1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > IP-Blocklist** aus.


Allgemein
Aktionen
A custom database of IP addresses from which you never want to receive emails.
IP-Blocklist aktivieren
IP-Blocklist-Eintrag
Einzelner Computer/CIDR
IP-Adresse:
Gruppe von Computern
Subnetzadresse:
Subnetzmaske
Beschreibung
Hinzufügen
IP-Blocklist
Adresse
Maske
Beschreibung
Es sind keine Datensätze zur Anzeige vorhanden.
Entfernen
Wenn Perimeterserver konfiguriert werden, ist die verifizierte IP-Adresse diejenige, die Daten an die Perimetergeräte sendet. Wenn keine Perimeterserver konfiguriert sind, ist die verifizierte IP-Adresse die IP-Adresse des Servers, der die Daten an GFI MailEssentials sendet.

Screenshot 68: IP-Blocklist

2. Wählen Sie auf der Registerkarte **Allgemein** die Option **IP-Blocklist aktivieren**, um alle E-Mails von bestimmten IP-Adressen zu blockieren.

3. Geben Sie im Feld **IP-Blocklist-Eintrag** die zu blockierenden IP-Adressen an:

Option	Beschreibung
Einzelner Computer/CIDR	Geben Sie eine einzelne IP-Adresse oder einen Bereich von IP-Adressen in der CIDR-Notation ein.
Gruppe von Computern	Geben Sie die **Subnetzadresse** und die **Subnetzmaske** der Gruppe von IP-Adressen an, die der Whitelist hinzugefügt werden soll. 2. Geben Sie eine **Beschreibung** ein (optional). 3. Klicken Sie auf **Hinzufügen**.
Beschreibung	Geben Sie optional eine Beschreibung ein, um die jeweiligen IP-Adressen zu identifizieren.

4. Klicken Sie auf **Hinzufügen**, um dem Feld **IP-Blocklist** spezifizierte IP-Adressen hinzuzufügen.

5. Um IP-Adressen aus der IP-Blocklist zu entfernen, wählen Sie die zu entfernende Adresse aus, und klicken Sie auf **Entfernen**.

6. Klicken Sie auf die Registerkarte **Aktionen**, um auszuwählen, was mit Nachrichten geschehen soll, die als Spam identifiziert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

> **HINWEIS**
>
> Wenn die IP-Blocklist für die Ausführung auf SMTP-Ebene konfiguriert wurde, ist auf der Registerkarte **Aktionen** nur die Option **Regelereignis in dieser Datei protokollieren** verfügbar.

7. Klicken Sie auf **Übernehmen**.

6.1.6 IP-DNS-Blocklist

Die IP-DNS-Blocklist vergleicht die IP-Adressen der sendenden Mailserver mit einer öffentlichen Liste von Mailservern, die bekanntermaßen Spam versenden. GFI MailEssentials unterstützt eine Reihe von IP-DNS-Blocklists. Verschiedene Drittanbieter stellen IP-DNS-Blocklists zur Verfügung. Darunter gibt es zuverlässige Listen – mit klar erläuterten Verfahren für die Aufnahme in oder das Ausscheiden aus der IP-DNS-Blocklist – und auch weniger zuverlässige Listen.

GFI MailEssentials speichert die Ergebnisse der Abfragen an die IP-DNS-Blocklists in einem Cache, um wiederholte Abfragen für dieselben IP-Adressen zu vermeiden. Die Einträge bleiben 4 Tage lang im Cache und werden bei einem Dienstneustart der GFI MailEssentials AS-Scan-Engine gelöscht.

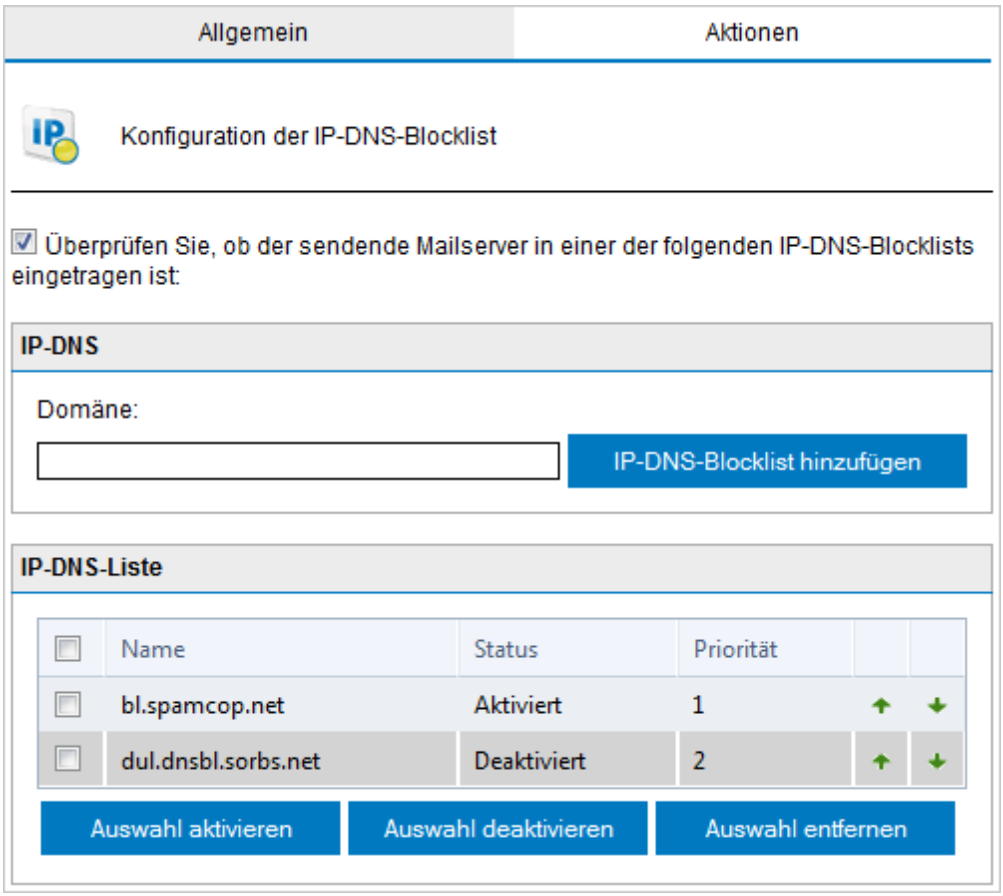
Dieser Filter kann so konfiguriert werden, dass er entweder beim Empfang der vollständigen E-Mail ausgeführt wird, oder dass er eingehende E-Mails auf SMTP-Ebene filtert. Bei der Filterung auf SMTP-Ebene wird die Verbindung zur E-Mail getrennt und somit das Herunterladen der vollständigen E-Mail gestoppt. Dies spart Bandbreite und Verarbeitungsressourcen. Die Verbindung wird in diesem Fall sofort getrennt, und die E-Mail muss keine weiteren Anti-Spam-Filter durchlaufen. Weitere Informationen finden Sie unter „SMTP-Übertragungsfilterung“ (Seite 154).

Dieser Filter wird bei der Installation von GFI MailEssentials standardmäßig aktiviert.

> **Wichtige Hinweise**
>
> 1. Für diese Funktion muss der DNS-Server korrekt konfiguriert sein. Ist dies nicht der Fall, kommt es zu Zeitüberschreitungen, die den E-Mail-Verkehr verzögern. Weitere Informationen finden Sie unter: http://go.gfi.com/?pageid=ME_ProcessingSlow
>
> 2. Abfragen an eine IP-DNS-Blocklist können eine gewisse Zeit in Anspruch nehmen (je nach Internet-Anbindung). Der E-Mail-Versand kann daher etwas verlangsamt werden.
>
> 3. Stellen Sie sicher, dass alle Perimeter-SMTP-Server im entsprechenden Dialogfeld konfiguriert wurden, damit GFI MailEssentials die IP-Adressen prüfen kann, die eine Verbindung mit den Perimeter-Servern herstellen. Weitere Informationen finden Sie unter „Perimeter-SMTP-Servereinstellungen“ (Seite 164).

Konfigurieren der IP-DNS-Blocklist

1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > IP-DNS-Blocklist** aus.



Screenshot 69: IP-DNS-Blocklist

2. Konfigurieren Sie die folgenden Optionen:

Option	Beschreibung
Überprüfen, ob der sendende Mailserver in einer der folgenden IP-DNS-Blocklists eingetragen ist:	Wählen Sie diese Option aus, um den IP-DNS-Blocklist-Filter zu aktivieren.
IP-DNS-Blocklist hinzufügen	Fügen Sie bei Bedarf weitere IP-DNS-Blocklists zu den bereits vorhandenen hinzu. Geben Sie die IP-DNS-Blocklist-Domäne ein, und klicken Sie auf **IP-DNS-Blocklist hinzufügen**.
Auswahl aktivieren	Wählen Sie eine IP-DNS-Blocklist aus, und klicken Sie auf **Auswahl aktivieren**, um sie zu aktivieren.
Auswahl deaktivieren	Wählen Sie eine IP-DNS-Blocklist aus, und klicken Sie auf **Auswahl deaktivieren**, um sie zu deaktivieren.
Auswahl entfernen	Wählen Sie eine IP-DNS-Blocklist aus, und klicken Sie auf **Auswahl entfernen**, um sie zu entfernen.

3. Klicken Sie auf die Registerkarte **Aktionen**, um auszuwählen, was mit Nachrichten geschehen soll, die als Spam identifiziert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

4. Klicken Sie auf **Übernehmen**.

HINWEIS

Um die IP-DNS-Blocklist auf Ebene des SMTP-Übertragungsfilters zu aktivieren, wählen Sie die Registerkarte **Anti-Spam > Filterpriorität > SMTP-Übertragungsfilter** und klicken Sie auf **Wechseln** neben der IP-DNS-Blockist, um das Filtern auf SMTP-Ebene oder bei Empfang der vollständigen E-Mail zu aktivieren/deaktivieren.

6.1.7 URI-DNS-Blocklist

Stoppt E-Mails, wenn sie Links zu Domänen enthalten, die in öffentlichen Spam-URI-Blocklists aufgeführt sind.

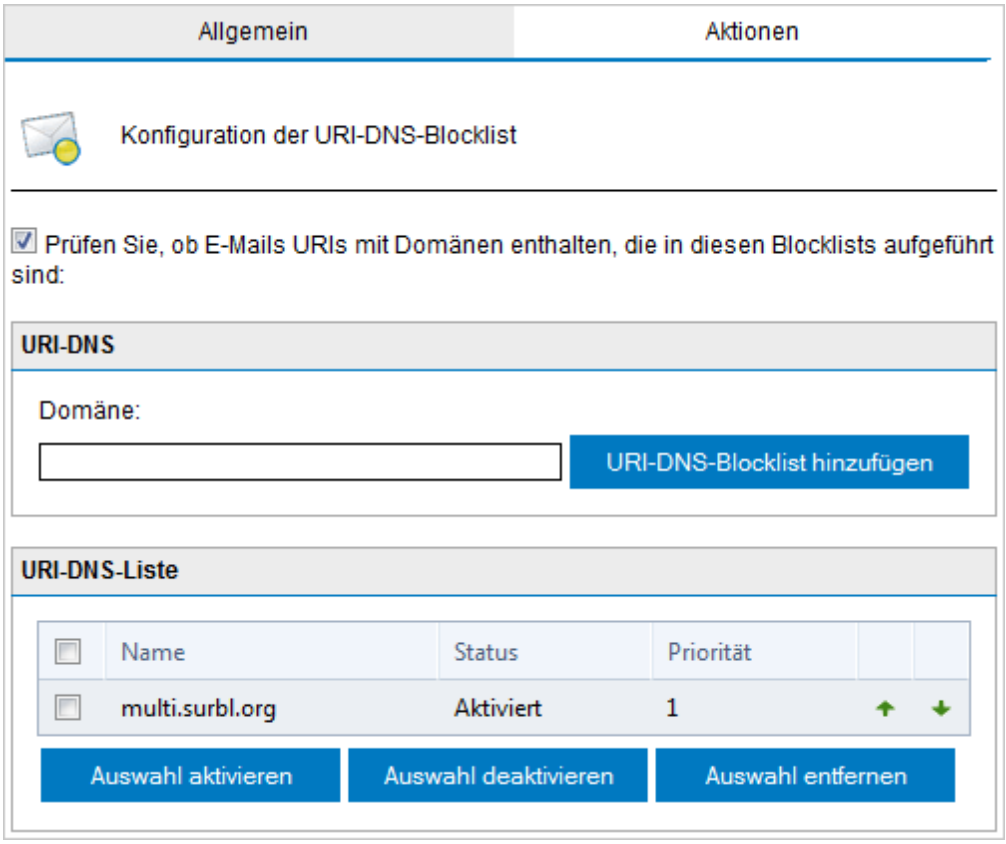
Ein Universal Resource Identifier (URI) besteht aus einer standardisierten Zeichenfolge, die der Adressierung von Ressourcen im WWW dient.

Realtime Blocklists (RBL) erkennen Spam anhand von Hyperlinks in einer E-Mail, die dafür bekannt sind, von Spammern verwendet zu werden.

Dieser Filter wird bei der Installation von GFI MailEssentials standardmäßig aktiviert.

Konfigurieren der URI-DNS-Blocklist

1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > URI-DNS-Blocklist** aus.



Screenshot 70: URI-DNS-Blocklist

2. Registerkarte **URI-DNS-Blocklist**:

Option	Beschreibung
Überprüfen, ob Mitteilungen URIs mit Domänen enthalten, die in diesen Blocklists verzeichnet sind:	Wählen Sie diese Option aus, um den URI-DNS-Blocklist-Filter zu aktivieren.

Option	Beschreibung
URI-DNS-Blocklist hinzufügen	Fügen Sie bei Bedarf weitere URI-DNS-Blocklists zu den bereits vorhandenen hinzu. Geben Sie die vollständige Domäne der URI-DNS-Blocklist ein, und klicken Sie auf **URI-DNS-Blocklist hinzufügen**.
Bevorzugte Reihenfolge	Die Reihenfolge der aktivierten URI-DNS-Blocklists kann geändert werden, indem Sie eine Blocklist auswählen und auf den Pfeil nach oben oder nach unten klicken.
Auswahl aktivieren	Wählen Sie eine URI-DNS-Blocklist aus, und klicken Sie auf **Auswahl aktivieren**, um sie zu aktivieren. **HINWEIS** Es wird empfohlen, alle anderen URI-DNS-Blocklists zu deaktivieren, wenn Sie **multi.surbl.org** aktivieren, da es ansonsten zu Verzögerungen bei der E-Mail-Verarbeitung kommen kann.
Auswahl deaktivieren	Wählen Sie eine URI-DNS-Blocklist aus, und klicken Sie auf **Auswahl deaktivieren**, um sie zu deaktivieren.
Auswahl entfernen	Wählen Sie eine URI-DNS-Blocklist aus, und klicken Sie auf **Auswahl entfernen**, um sie zu entfernen.

3. Klicken Sie auf die Registerkarte **Aktionen**, um auszuwählen, was mit Nachrichten geschehen soll, die als Spam identifiziert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

4. Klicken Sie auf **Übernehmen**.

6.1.8 Sender Policy Framework

Dieser Filter blockiert E-Mails von gefälschten IP-Adressen, indem er mithilfe von SPF-Einträgen prüft, ob die jeweilige Absender-IP-Adresse autorisiert ist. Der Sender Policy Framework-Filter basiert auf einer gemeinschaftlichen Zusammenarbeit, bei der die Absender die IP-Adressen ihrer Mailserver in einem SPF-Eintrag veröffentlichen.

Beispiel: Wird eine E-Mail von xyz@UnternehmenABC.com verschickt, muss Unternehmen ABC einen SPF-Eintrag veröffentlicht haben, damit SPF feststellen kann, ob die E-Mail wirklich aus dem Netzwerk von Unternehmen ABC versendet wurde oder ob sie gefälscht ist. Hat Unternehmen ABC keinen SPF-Eintrag veröffentlicht, wird als Ergebnis der SPF-Abfrage ‘unknown’ ausgegeben.

Weitere Informationen zu SPF und der genauen Funktionsweise finden Sie auf der Sender Policy Framework-Website:

http://www.openspf.org.

Der SPF-Filter ist NICHT standardmäßig aktiviert, aber es wird empfohlen, diese Option zu aktivieren und den Filter vor der E-Mail-Whitelist-Prüfung auszuführen, damit gefälschte Absender blockiert werden und nicht in die Whitelist gelangen.

Um diese Funktion von GFI MailEssentials nutzen zu können, müssen Sie nicht zwingend SPF-Einträge veröffentlichen. Wenn Sie jedoch SPF-Einträge veröffentlichen möchten, können Sie hierfür den SPF-Assistenten verwenden:

http://www.openspf.org/wizard.html.

Voraussetzungen

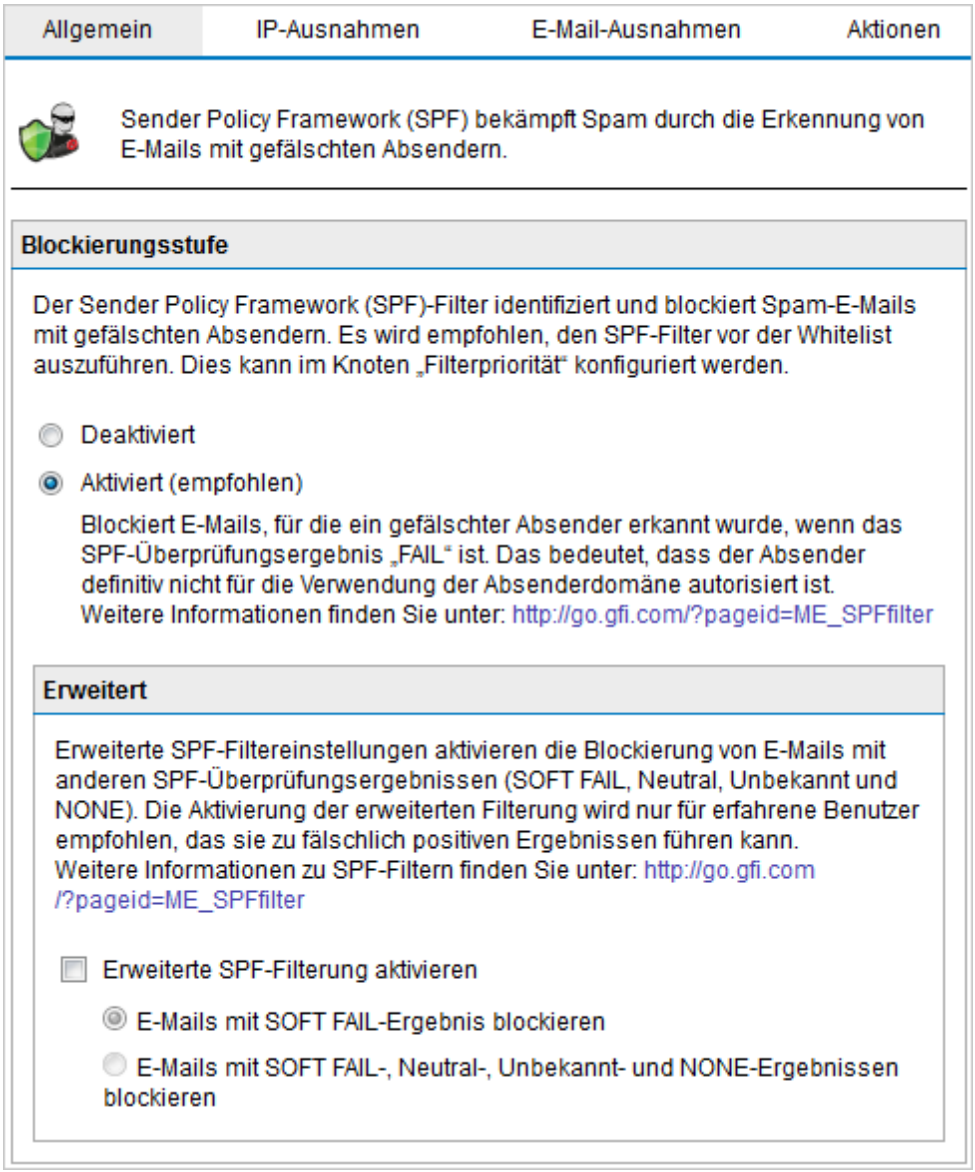
Haben Sie die Installation nicht auf einem Gateway-Server durchgeführt, gehen Sie wie folgt vor, bevor Sie den Sender Policy Framework-Filter aktivieren:

1. Klicken Sie auf **Anti-Spam > Anti-Spam-Einstellungen**, und wählen Sie die Registerkarte für Perimeter-SMTP-Server aus.

2. Klicken Sie in der Perimeter-SMTP-Einrichtungsoption auf **Erkennen**, um eine DNS-MX-Suche auszuführen und die IP-Adresse Ihres Perimeter-SMTP-Servers automatisch zu definieren.

Aktivieren des Sender Policy Framework

1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > Sender Policy Framework** aus.


Allgemein
IP-Ausnahmen
E-Mail-Ausnahmen
Aktionen
Sender Policy Framework (SPF) bekämpft Spam durch die Erkennung von E-Mails mit gefälschten Absendern.
Blockierungsstufe
Der Sender Policy Framework (SPF)-Filter identifiziert und blockiert Spam-E-Mails mit gefälschten Absendern. Es wird empfohlen, den SPF-Filter vor der Whitelist auszuführen. Dies kann im Knoten „Filterpriorität" konfiguriert werden.
Deaktiviert
Aktiviert (empfohlen)
Blockiert E-Mails, für die ein gefälschter Absender erkannt wurde, wenn das SPF-Überprüfungsergebnis „FAIL" ist. Das bedeutet, dass der Absender definitiv nicht für die Verwendung der Absenderdomäne autorisiert ist.
Weitere Informationen finden Sie unter: http://go.gfi.com/?pageid=ME_SPFfilter
Erweitert
Erweiterte SPF-Filtereinstellungen aktivieren die Blockierung von E-Mails mit anderen SPF-Überprüfungsergebnissen (SOFT FAIL, Neutral, Unbekannt und NONE). Die Aktivierung der erweiterten Filterung wird nur für erfahrene Benutzer empfohlen, das sie zu fälschlich positiven Ergebnissen führen kann.
Weitere Informationen zu SPF-Filtern finden Sie unter: http://go.gfi.com/?pageid=ME_SPFfilter
Erweiterte SPF-Filterung aktivieren
E-Mails mit SOFT FAIL-Ergebnis blockieren
E-Mails mit SOFT FAIL-, Neutral-, Unbekannt- und NONE-Ergebnissen blockieren

Screenshot 71: Sender Policy Framework aktivieren und konfigurieren

2. Klicken Sie auf **Aktiviert**, um den Sender Policy Framework-Filter zu aktivieren. Ist die IP-Adresse eines E-Mail-Absenders definitiv nicht berechtigt, E-Mails von der Absenderdomäne zu verschicken, werden diese E-Mails blockiert.

3. Wählen Sie optional die Option **Erweiterte SPF-Filterung aktivieren** aus, und wählen Sie eine der erweiterten Optionen aus:

OPTION	BESCHREIBUNG
E-Mails mit SOFT FAIL-Ergebnis blockieren	Alle E-Mails blockieren, für die Folgendes zutrifft: » Die IP-Adresse des Absenders ist definitiv nicht berechtigt, E-Mails von der Absenderdomäne zu verschicken. » Die IP-Adresse des Absenders ist wahrscheinlich nicht berechtigt, E-Mails von der Absenderdomäne zu verschicken. Weitere Informationen zur erweiterten SPF-Filterung finden Sie unter: http://go.gfi.com/?pageid=ME_SPFfilter
E-Mails mit SOFT FAIL-, Neutral-, Unbekannt- und NONE-Ergebnissen blockieren	Alle E-Mails blockieren, für die Folgendes zutrifft: » Die IP-Adresse des Absenders ist definitiv nicht berechtigt, E-Mails von der Absenderdomäne zu verschicken. » Die IP-Adresse des Absenders ist wahrscheinlich nicht berechtigt, E-Mails von der Absenderdomäne zu verschicken. » Die IP-Adresse des Absenders ist explizit uneindeutig oder unbekannt, oder es wurden keine Daten dazu veröffentlicht. Weitere Informationen zur erweiterten SPF-Filterung finden Sie unter: http://go.gfi.com/?pageid=ME_SPFfilter

4. Wählen Sie die Registerkarte **IP-Ausnahmen** oder **E-Mail-Ausnahmen** aus, um IP-Adressen und/oder Empfänger zu konfigurieren, die von SPF-Überprüfungen ausgeschlossen werden sollen:

» **IP-Ausnahmeliste:** Einträge in dieser Liste werden bei SPF-Überprüfungen nicht berücksichtigt. Aktivieren Sie das Kontrollkästchen **IP-Ausnahmeliste**, fügen Sie eine neue IP-Adresse und eine Beschreibung hinzu, und klicken Sie auf **Hinzufügen**. Wählen Sie zum Entfernen von Einträgen diese aus der Liste aus, und klicken Sie auf **Auswahl entfernen**. Um die IP-Ausnahmeliste zu deaktivieren, deaktivieren Sie das Kontrollkästchen **IP-Ausnahmeliste**.

> **HINWEIS**
>
> Beim Hinzufügen von IP-Adressen zur IP-Ausnahmeliste können Sie auch einen Bereich von IP-Adressen in CIDR-Notation eingeben.

» **E-Mail-Ausnahmeliste:** Mit dieser Option wird sichergestellt, dass bestimmte Absender oder Empfänger von E-Mails von SPF-Prüfungen ausgenommen werden; dies gilt auch für abgelehnte Nachrichten. Aktivieren Sie das Kontrollkästchen **E-Mail-Ausnahmeliste**, fügen Sie eine neue E-Mail-Adresse und eine Beschreibung hinzu, und klicken Sie auf **Hinzufügen**. Wählen Sie zum Entfernen von Einträgen diese aus der Liste aus, und klicken Sie auf **Auswahl entfernen**. Um die E-Mail-Ausnahmeliste zu deaktivieren, deaktivieren Sie das Kontrollkästchen **E-Mail-Ausnahmeliste**. E-Mail-Adressen können wie folgt eingegeben werden:

- Lokaler Bereich – z. B. ‘Verstoß’ (entspricht ‘Verstoß@abc.com’, ‘Verstoß@xyz.com’ usw.)
- Domäne – z. B. ‘@abc.com’ (entspricht ‘john@abc.com’, ‘jill@abc.com’ usw.)
- Vollständige Adresse – z. B. ‘joe@abc.com’ (entspricht nur ‘joe@abc.com’)

5. Klicken Sie auf die Registerkarte **Aktionen**, um auszuwählen, was mit Nachrichten geschehen soll, die als Spam identifiziert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

6. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

6.1.9 Anti-Spoofing

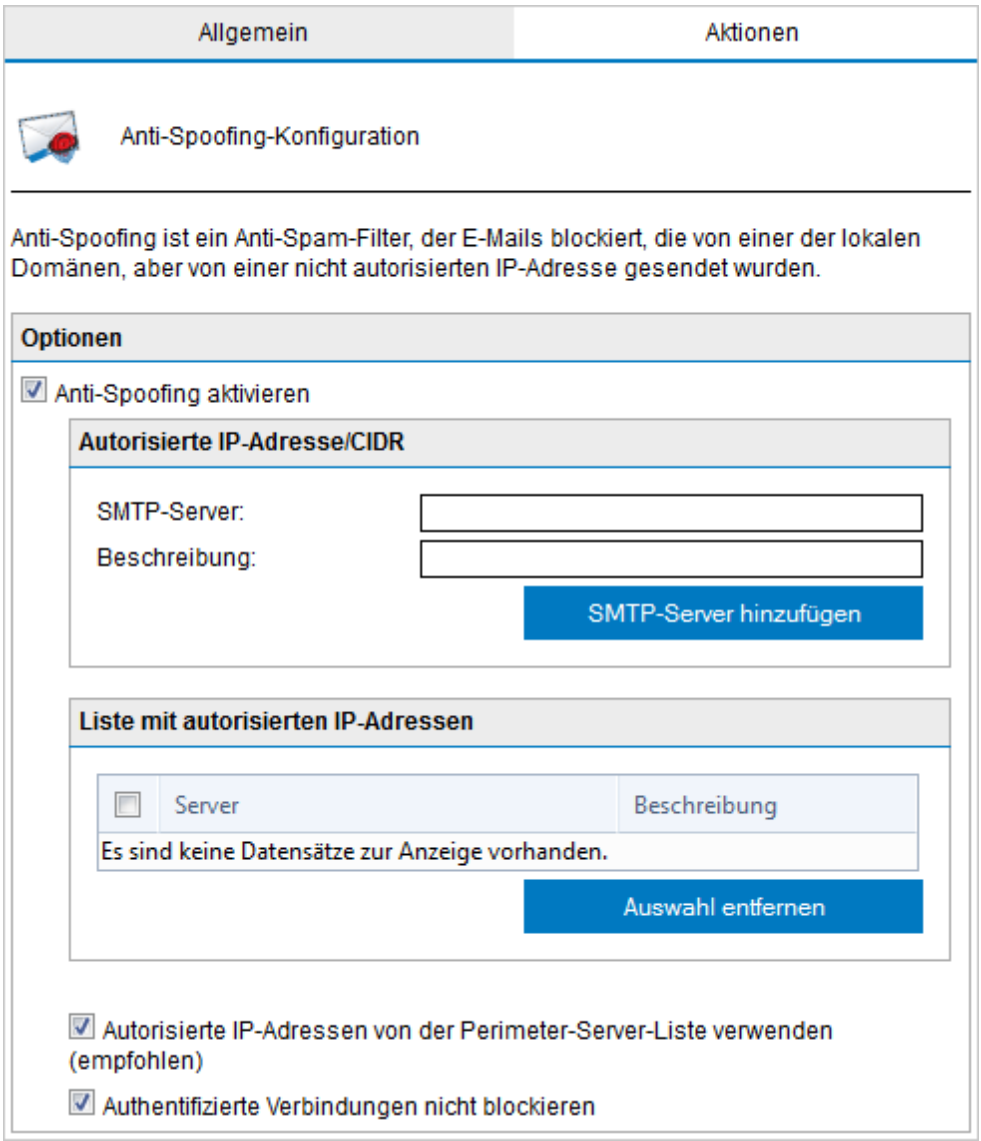
Dieser Filter vergleicht E-Mails, deren Absenderadresse mit Ihrer eigenen Domäne übereinzustimmen scheint, mit einer Liste von IP-Adressen in GFI MailEssentials. Befindet sich die Absender-IP-Adresse nicht in der Liste mit den Server-IP-Adressen der eigenen Domäne, wird die E-Mail blockiert.

Dieser Filter ist NICHT standardmäßig aktiviert.

> **WARNHINWEIS**
>
> Wenn Sie diese Funktion aktivieren, sollten Sie keine internen Benutzer auf die Whitelist setzen, da es den Zweck der Anti-Spoofing-Prüfung verfehlt.

Aktivieren und Konfigurieren von Anti-Spoofing

1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > Anti-Spoofing** aus.



Screenshot 72: GFI MailEssentials Anti-Spoofing-Filter

2. Wählen Sie **Anti-Spoofing aktivieren**, um den Anti-Spoofing-Filter zu aktivieren.

3. Geben Sie im Feld **SMTP-Server:** den SMTP-Server an, auf dem GFI MailEssentials nach E-Mail-Empfängeradressen sucht. Geben Sie im Feld **Beschreibung:** auch eine Beschreibung für den Server ein.

HINWEIS

Der SMTP-Server kann im entsprechenden Feld wie folgt angegeben werden:

» Als einzelne IP-Adresse

» Als CIDR-Bereich (z. B. 192.0.2.1/24)

4. Klicken Sie auf **SMTP-Server hinzufügen**, um die Angaben zum SMTP-Server zu speichern.

HINWEIS

Zum Entfernen zuvor hinzugefügter SMTP-Server wählen Sie einen SMTP-Server aus der Liste mit autorisierten IP-Adressen aus und klick Sie auf **Auswahl entfernen**.

Die Optionen **Autorisierte IP-Adressen von der Perimeter-Server-Liste verwenden** und **Authentifizierte Verbindungen nicht blockieren** sind standardmäßig aktiviert. Diese Options sollten nicht deaktiviert werden.

HINWEIS

Das Kontrollkästchen **Authentifizierte Verbindungen nicht blockieren** gilt nicht für Microsoft IIS und Microsoft Exchange 2003. Es funktioniert nur mit Exchange 2007 oder neuer.

6.1.10 Greylist

Der Greylist-Filter blockiert temporär eingehende E-Mails von unbekannten Absendern. Zulässige Mailsysteme versuchen normalerweise, die E-Mail nach einigen Minuten erneut zu senden, Spammer hingegen ignorieren solche Fehlernachrichten einfach. Falls innerhalb eines festgelegten Zeitraums erneut eine E-Mail empfangen wird, führt die Greylist Folgendes durch:

» Die Daten des Absenders werden in einer Datenbank gespeichert, so dass bei einer erneuten E-Mail von diesem Absender diese nicht auf die Greylist gelangt.

» Die E-Mail wird empfangen und einer Spam-Prüfung unterzogen.

Die Greylist ist standardmäßig **DEAKTIVIERT**.

Wichtige Hinweise

1. Um die Greylist zu aktivieren, muss GFI MailEssentials auf dem Perimeter-SMTP-Server installiert sein. Weitere Informationen finden Sie unter http://go.gfi.com/?pageid=ME_GreylistSMTP

2. Die Greylist enthält Ausnahmelisten, so dass bestimmte E-Mail-Adressen, Domänen und IP-Adressen nicht auf die Greylist gesetzt werden. Ausnahmen können in folgenden Situationen konfiguriert werden:

» Wenn E-Mails von bestimmten E-Mail-Adressen, Domänen oder IP-Adressen nicht verzögert werden dürfen

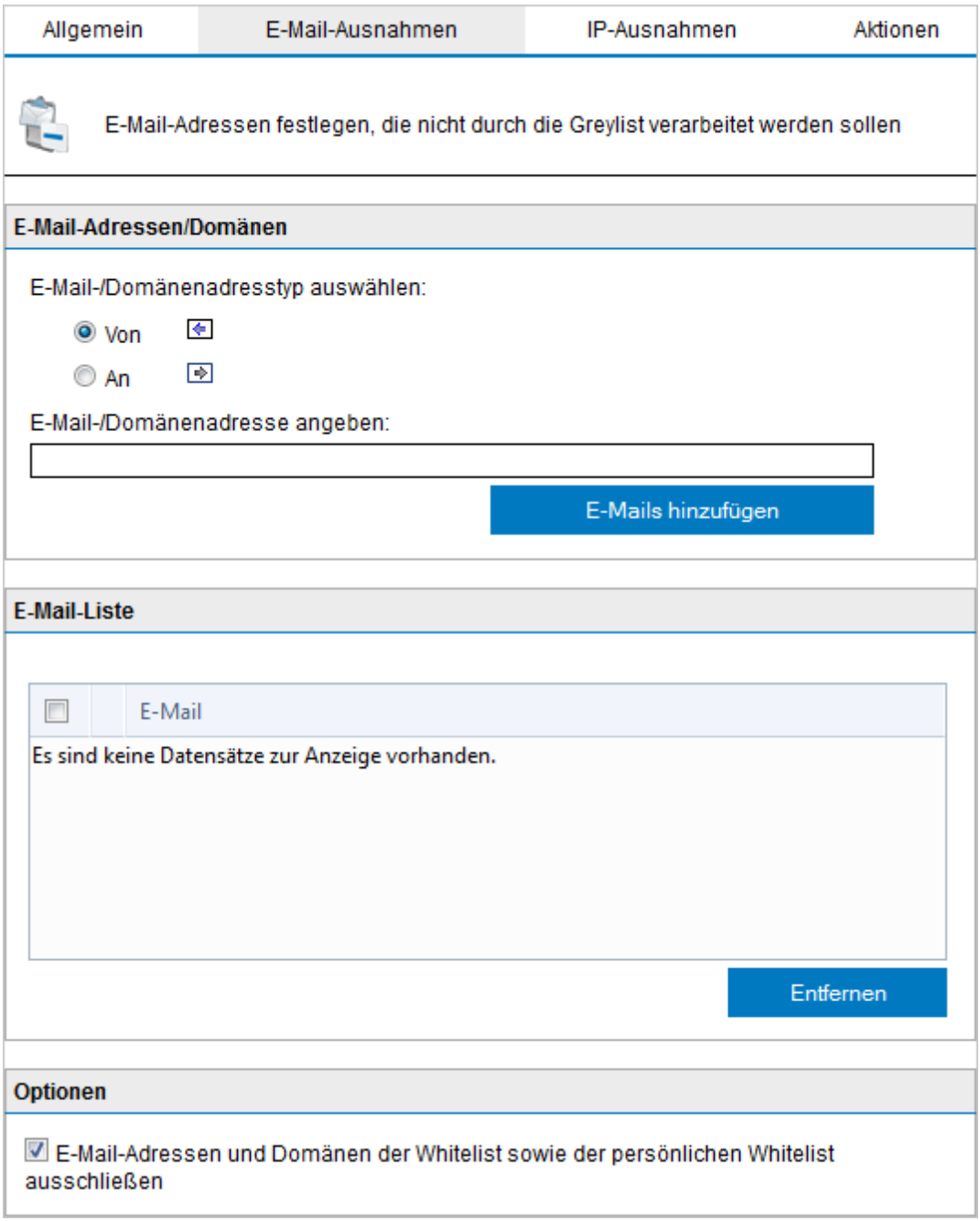
» Wenn E-Mails an einen bestimmten lokalen Benutzer nicht verzögert werden dürfen

Konfigurieren der Greylist

1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > Greylist** aus.

2. Aktivieren/deaktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Greylist**

aktivieren, um die Greylist zu aktivieren oder zu deaktivieren.



Screenshot 73: E-Mail-Ausnahmen

3. Legen Sie auf der Registerkarte **E-Mail-Ausnahmen** die E-Mail-Adressen und Domänen fest, die nicht auf der Greylist erscheinen sollen. Geben Sie im Bereich **E-Mail-Adressen** Folgendes an:

» eine vollständige E-Mail-Adresse oder

» E-Mails von einer ganzen Domäne (z. B.: *@trusteddomain.com) oder

» eine ganze Top-Level-Domäne (z. B.: *@*.mil oder *@*.edu)

Legen Sie auch fest, ob sich die Ausnahme auf Absender (**Von (>)**) oder lokale Empfänger (**An (>)**) beziehen soll.

» **Beispiel 1:** E-Mails mit dem Empfänger administrator@mydomain.com sollen nicht auf die Greylist gesetzt werden, damit E-Mails an diesen Empfänger nie verzögert werden.

» **Beispiel 2:** E-Mails mit der Absenderdomäne trusteddomain.com (`*@trusteddomain.com`) sollen nicht auf die Greylist gesetzt werden, damit E-Mails von dieser Domäne nie verzögert werden.

Klicken Sie auf **E-Mails hinzufügen**, um die Ausnahme hinzuzufügen.

> **HINWEIS**
>
> Um E-Mail-Adressen und Domänen aus der Whitelist von der Greylist und den damit verbundenen Verzögerungen auszuschließen, wählen Sie **E-Mail-Adressen und Domänen der Whitelist ausschließen** aus.

4. Wählen Sie die Registerkarte **IP-Ausnahmen** aus, um bestimmte IP-Adressen von der Greylist auszuschließen. Klicken Sie auf **Hinzufügen…**, und geben Sie eine IP-Adresse an, die ausgeschlossen werden soll.

5. Um IP-Adressen aus der Whitelist von der Greylist und den damit verbundenen Verzögerungen auszuschließen, wählen Sie **IP-Adressen der Whitelist ausschließen** aus.

6. Um Greylist-Ereignisse in einer Protokolldatei zu speichern, wählen Sie auf der Registerkarte **Aktionen** die Option **Regelereignis in dieser Datei protokollieren** aus.

> **HINWEIS**
>
> Protokolldateien können sehr groß werden. GFI MailEssentials bietet einen Protokollrotator, durch den in regelmäßigen Abständen oder bei Erreichen einer bestimmten Größe eine neue Protokolldatei erstellt wird. Um den Protokollrotator zu aktivieren, öffnen Sie **Anti-Spam > Anti-Spam-Einstellungen**. Aktivieren Sie auf der Registerkarte **Anti-Spam-Protokollierung** die Option **Protokollrotator aktivieren**, und legen Sie die Rotationsbedingungen fest.

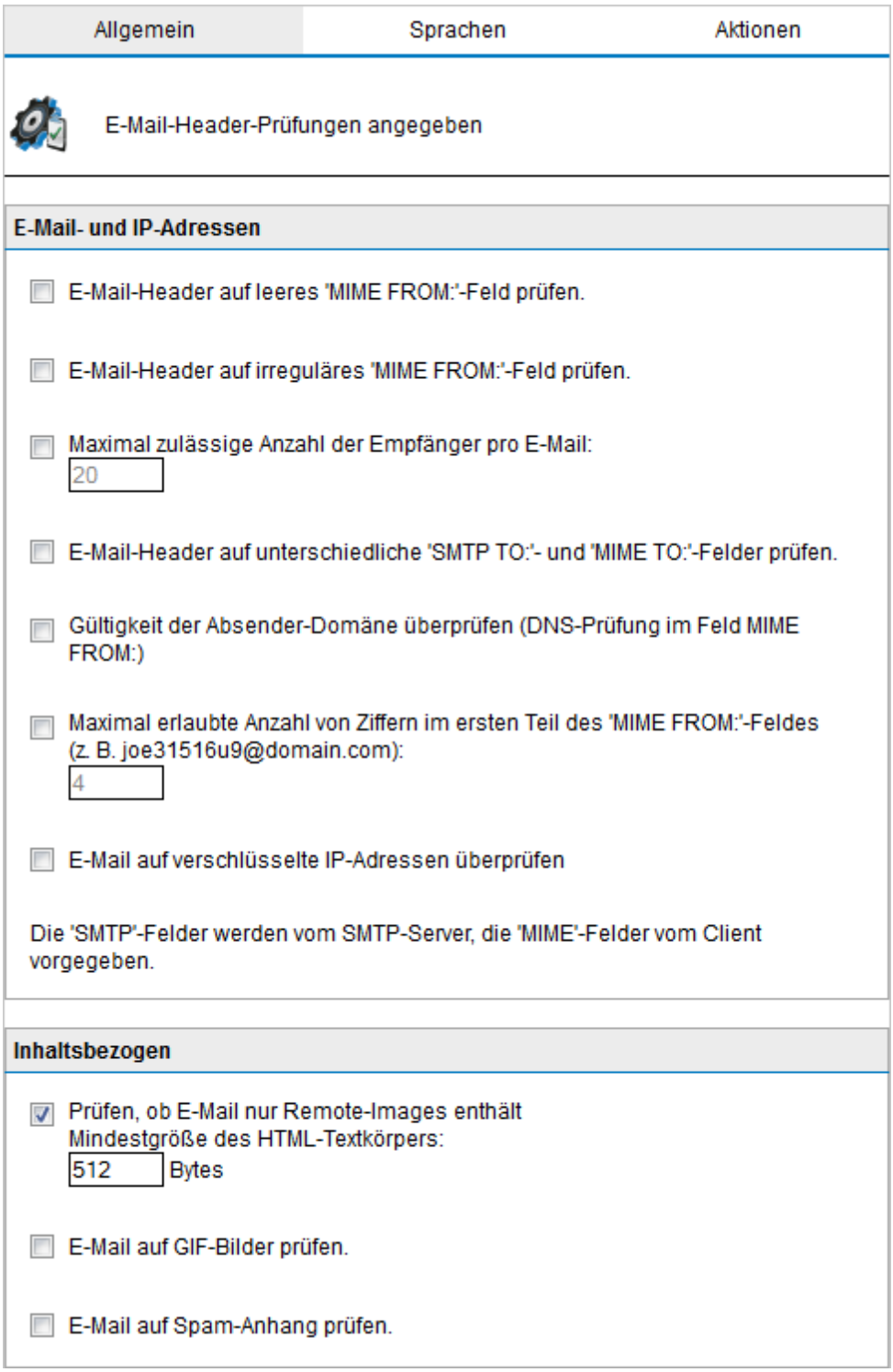
7. Klicken Sie auf **Übernehmen**.

6.1.11 Header-Prüfung

Der Filter zur Header-Kontrolle analysiert E-Mail-Header, um Spam-Mails zu erkennen.

Konfigurieren der Header-Prüfung

1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > Header-Prüfung** aus.


Allgemein
Sprachen
Aktionen
E-Mail-Header-Prüfungen angegeben
E-Mail- und IP-Adressen
E-Mail-Header auf leeres 'MIME FROM:'-Feld prüfen.
E-Mail-Header auf irreguläres 'MIME FROM:'-Feld prüfen.
Maximal zulässige Anzahl der Empfänger pro E-Mail:
20
E-Mail-Header auf unterschiedliche 'SMTP TO:'- und 'MIME TO:'-Felder prüfen.
Gültigkeit der Absender-Domäne überprüfen (DNS-Prüfung im Feld MIME FROM:)
Maximal erlaubte Anzahl von Ziffern im ersten Teil des 'MIME FROM:'-Feldes (z. B. joe31516u9@domain.com):
4
E-Mail auf verschlüsselte IP-Adressen überprüfen
Die 'SMTP'-Felder werden vom SMTP-Server, die 'MIME'-Felder vom Client vorgegeben.
Inhaltsbezogen
Prüfen, ob E-Mail nur Remote-Images enthält
Mindestgröße des HTML-Textkörpers:
512
Bytes
E-Mail auf GIF-Bilder prüfen.
E-Mail auf Spam-Anhang prüfen.

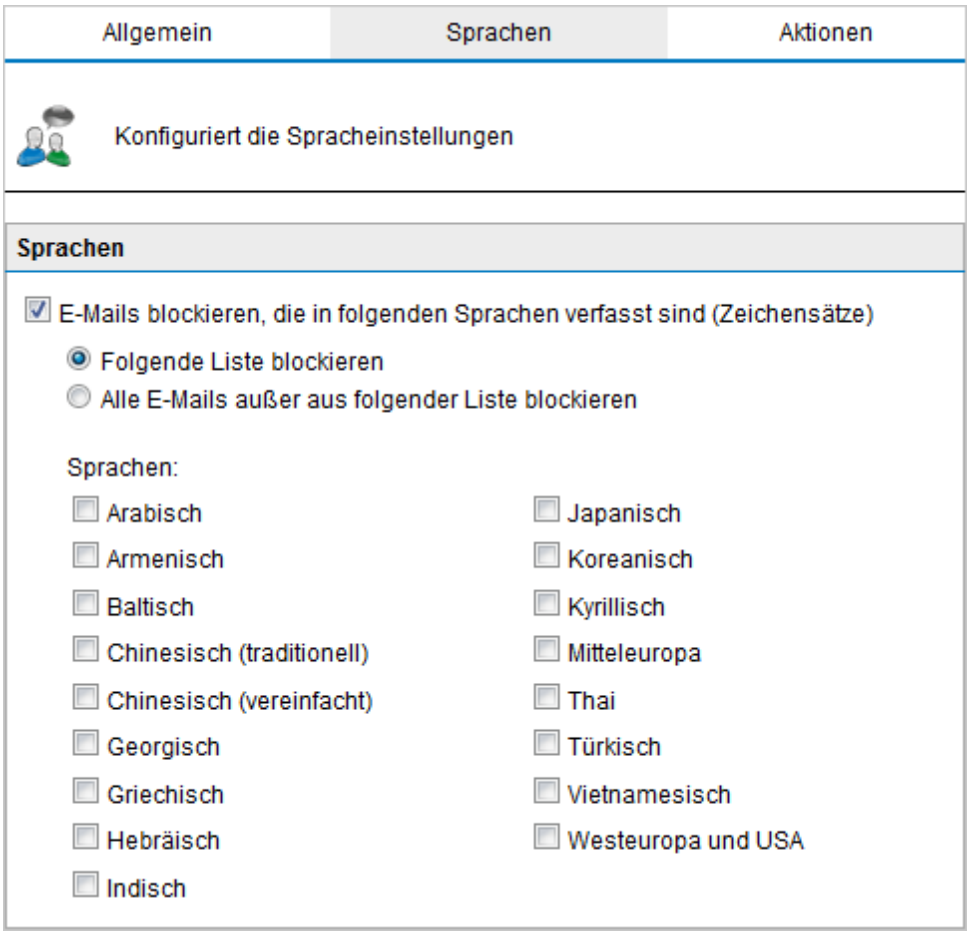
Screenshot 74: Optionen der Header-Prüfung

2. Aktivieren, deaktivieren oder konfigurieren Sie folgende Optionen:

Option	Beschreibung
E-Mail-Header auf leeres 'MIME FROM:'-Feld prüfen	Prüft, ob der Absender der E-Mail seinen Namen im FROM:-Feld angegeben hat. Wenn das Feld leer ist, wird die Nachricht als SPAM gekennzeichnet.
E-Mail-Header auf irreguläres 'MIME FROM:'-Feld prüfen	Überprüft den MIME-Typ, ob dieser gemäß RFC definiert ist.

Option	Beschreibung
Maximal zulässige Anzahl der Empfänger pro E-Mail	Ermittelt E-Mails mit einer großen Anzahl an Empfängern und kennzeichnet sie als SPAM.
E-Mail-Header auf unterschiedliche 'SMTP TO:'- und 'MIME TO:'-Felder prüfen	Überprüft, ob die Angaben in den „SMTP TO:“- und „MIME TO:“-Feldern übereinstimmen. Der E-Mail-Server eines Spammers muss immer eine SMTP TO-Adresse angeben. Die MIME TO-Adresse wird jedoch oftmals nicht mit angegeben oder unterscheidet sich von der SMTP TO-Adresse. **HINWEIS:** Durch Aktivierung dieser Funktion können viele Spam-Mitteilungen abgefangen werden. Dabei ist jedoch zu beachten, dass die MIME TO-Adresse auch von einigen Listen-Servern nicht angegeben wird. Daher sollten die Absenderadressen von Newslettern bei Verwendung dieser Funktion in die Whitelist aufgenommen werden.
Gültigkeit der Absender-Domäne überprüfen (DNS-Prüfung im Feld MIME FROM:)	Führt eine DNS-Überprüfung der im MIME FROM-Feld angegebenen Domäne durch und stellt fest, ob sie gültig ist. **HINWEIS:** Stellen Sie sicher, dass der DNS-Server ordnungsgemäß konfiguriert ist, um Zeitüberschreitungen und einen langsamen E-Mail-Fluss zu vermeiden.
Maximal erlaubte Anzahl von Ziffern im ersten Teil des 'MIME FROM:'-Feldes:	Erkennt das Vorhandensein von Zahlen im MIME FROM-Feld. Spammer verwenden oft Tools, die automatisch eine unverwechselbare Antwortadresse erstellen, in der Zahlen verwendet werden.
E-Mail auf verschlüsselte IP-Adressen überprüfen	Sucht im Nachrichten-Header und Textkörper nach URLs, die eine hexadezimal/oktal verschlüsselte IP (http://0072389472/hello.com) aufweisen oder eine Kombination aus Benutzername/Passwort enthalten (z. B. www.citibank.com@scammer.com). Die folgenden Beispiele werden als Spam gekennzeichnet: » http://12312 » www.microsoft.com:hello%01@123123
Prüfen, ob E-Mail nur Remote-Images enthält Mindestgröße des HTML-Textkörpers	E-Mails werden als Spam klassifiziert, wenn sie fast nur aus Remote-Bildern und kaum aus Text bestehen. Diese Funktion wirkt unterstützend, um Bild-Spam zu erkennen.
E-Mail auf GIF-Bilder prüfen	Kontrolliert, ob eine E-Mail ein oder mehrere eingebettete Bilder im GIF-Format enthält. Bilder dieser Art werden häufig eingesetzt, um Spam-Filter zu überlisten. **WICHTIG:** **Da jedoch auch in erwünschten E-Mails GIF-Bilder verwendet werden können, sind bei Aktivierung dieser Option Fehlalarme möglich.**
E-Mail auf Spam-Anhang prüfen	Kontrolliert, ob an E-Mails angehängte Dateien Spam-typische Eigenschaften aufweisen. Dadurch kann mit den neuesten Techniken von Spammern Schritt gehalten werden, bei denen Spam als Dateinanhang versendet wird.
Kontrollieren, ob die Betreffzeile den ersten Teil der Empfänger-Adresse enthält	Erkennt personalisierte Spam-Mails, bei denen der vor dem @-Zeichen stehende Benutzername des Empfängers oft in der Betreffzeile eingesetzt wird.

3. Wählen Sie auf der Registerkarte **Sprache** die Option **E-Mails blockieren, die diese Sprachen verwenden** aus, um die Spracherkennung zu aktivieren.



Screenshot 75: Spracherkennung

4. Wählen Sie **Folgende Liste blockieren** aus, um die zu blockierenden Sprachen auszuwählen, oder **Alle E-Mails außer aus folgender Liste blockieren**, um alle Sprachen mit Ausnahme der ausgewählten zu blockieren.

5. Wählen Sie die Sprachen, die blockiert bzw. zugelassen werden sollen, im Bereich **Sprachen** aus.

6. Klicken Sie auf die Registerkarte **Aktionen**, um auszuwählen, was mit Nachrichten geschehen soll, die als Spam identifiziert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

7. Klicken Sie auf **Übernehmen**.

6.1.12 Spam-Stichwortprüfung

Dieser Filter ermöglicht die Erkennung von Spam auf der Basis von Stichwörtern in eingehenden E-Mails.

Dieser Filter wird **NICHT** standardmäßig bei der Installation von GFI MailEssentials aktiviert.

> **HINWEIS**
>
> Dieser Filter überprüft den Inhalt einer E-Mail nur auf Text, der sie als Spam identifiziert. Für eine umfassende Inhaltsfilterung von E-Mails (z. B. um rassistische oder anstößige Inhalte zu blockieren) verwenden Sie die Stichwortfilteroption der Inhaltsfilterung.

Spam-Stichwortprüfung hinzufügen

1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > Spam-Stichwortprüfung** aus.

2. Wählen Sie auf der Registerkarte **Textkörper** die Option **E-Mails blockieren, wenn der Inhalt (Nachrichtentext) diese Bedingungen erfüllt**, um die Spam-Stichwortprüfung für den E-Mail-Text zu aktivieren.

Textkörper
Betreff
Aktionen
Konfigurieren Sie Stichwortfilteroptionen für die Überprüfung des Nachrichtentextes.
E-Mails blockieren, wenn der Inhalt (Nachrichtentext) diese Bedingungen erfüllt
Bedingungseintrag
Bedingung bearbeiten:
AND
OR
AND NOT
OR NOT
Bedingung hinzufüge
Update
Bedingungsliste
Mithilfe des OR-Operators für jeden Eintrag werden alle diese Bedingungen als eine einzelne Bedingung geprüft. Durch Klicken auf einen Eintrag wird der Bedingungstext zur Bearbeitung in den obigen Bedingungseintrag kopiert.
Suche
Suche
Aktuelle Bedingungen:
Bedingung
uce-mail act
h.r. 3113
100% confidential
100% free
100% guaranteed
100% legal
1 2 3 4 5 6 7 8 9 10 ...
Seite 1 von 17, Elemente 1 bis 10 von 161.
Entfernen
Exportieren
Geben Sie den vollständigen Pfad und Dateinamen für den Import an:
Importieren
Hinweis: Der Import der Listendaten kann nur durchgeführt werden, wenn sich die zu importierende Liste auf dem gleichen Computer wie GFI MailEssentials befindet.

Screenshot 76: Eigenschaften der Spam-Stichwortprüfung

3. Geben Sie im Bereich **Bedingungseintrag** ein Stichwort oder eine Kombination von Stichwörtern ein, die dieser Filter blockieren soll. Verwenden Sie die Operatoren 'AND', 'OR', 'AND NOT' und 'OR

NOT', um spezifische Bedingungen zu konfigurieren.

Beispiel:

Wenn Sie beispielsweise ‘Basketball-Sport’ eingeben, blockiert GFI MailEssentials E-Mails, die diesen Ausdruck enthalten. Nur der gesamte Ausdruck wird diese Regel aktivieren, nicht aber die Wörter 'Basketball' oder 'Sport', wenn sie durch andere Wörter getrennt sind.

Wenn Sie 'Basketball AND Baseball' eingeben, blockiert GFI MailEssentials E-Mails, die beide Wörter enthalten. E-Mails, die nur das Wort 'Basketball' oder nur das Wort 'Baseball' enthalten, werden nicht blockiert.

4. Wählen Sie **Nur ganze Wörter berücksichtigen** aus, wenn nur nach bestimmten ganzen Wörtern gesucht werden soll. Wörter, die das betreffende Wort als Bestandteil enthalten, werden somit nicht blockiert. Wenn Sie beispielsweise das Wort 'Sex' blockieren möchten, wird mit dieser Option das Wort 'MSExchange' nicht blockiert, obwohl 'sex' darin enthalten ist.

5. Wählen Sie auf der Registerkarte **Betreff** die Option **E-Mails blockieren, wenn der Inhalt (Nachrichtenbetreff) diese Bedingungen erfüllt** aus, um die Spam-Stichwortprüfung für den E-Mail-Betreff zu aktivieren.

6. Geben Sie im Bereich **Bedingungseintrag** ein Stichwort oder eine Kombination von Stichwörtern ein, die dieser Filter blockieren soll. Verwenden Sie die Operatoren 'AND', 'OR', 'AND NOT' und 'OR NOT', um spezifische Bedingungen zu konfigurieren.

7. Wählen Sie **Liste mit Schlüsselwörtern auch zum Scannen der Anzeigenamen von Absendern verwenden** aus, um den Anzeigenamen des E-Mail-Absenders auf Spam-Stichwörter zu prüfen. Spam-Nachrichten zum Thema Viagra haben beispielsweise oft gefälschte Absender, die das Wort Viagra im Absender enthalten.

8. Klicken Sie auf die Registerkarte **Aktionen**, um auszuwählen, was mit Nachrichten geschehen soll, die als Spam identifiziert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

9. Klicken Sie auf **Übernehmen**.

Entfernen von Bedingungen

So entfernen Sie eine Bedingung für die Spam-Stichwortprüfung:

1. Wählen Sie auf der Registerkarte **Textkörper** oder **Betreff** im Bereich **Bedingungsliste** eine oder mehrere Bedingungen aus, die Sie entfernen möchten.

> **HINWEIS**
>
> Verwenden Sie zum Auffinden der gewünschten Bedingungen die Steuerelemente unter der Bedingungsliste, um in den Seiten zu blättern.

2. Klicken Sie auf **Entfernen** und dann auf **Übernehmen**.

Importieren und Exportieren von Bedingungen

So exportieren Sie mehrere Bedingungen:

1. Wählen Sie auf der Registerkarte **Textkörper** oder **Betreff** im Bereich **Bedingungsliste** eine oder mehrere Bedingungen aus, die Sie exportieren möchten.

HINWEIS

Verwenden Sie zum Auffinden der gewünschten Bedingungen die Steuerelemente unter der Bedingungsliste, um in den Seiten zu blättern.

2. Klicken Sie im Fenster **Datei herunterladen** auf **Speichern**, und wählen Sie einen Speicherort für die Exportdatei aus.

So importieren Sie Bedingungen:

1. Geben Sie im Bereich **Bedingungen** auf der Registerkarte **Textkörper** oder **Betreff** den Ordner- und Dateinamen der Datei ein, die importiert werden soll.

2. Klicken Sie auf **Importieren**.

6.1.13 Bayes'sche Analyse

Ein Anti-Spam-Filter kann so trainiert werden, dass er auf der Basis von Erfahrungswerten genau bestimmen kann, ob es sich bei einer E-Mail um Spam handelt.

In diesem Handbuch wird erläutert, wie der Bayes'sche Filter funktioniert und wie er trainiert wird. Weitere Informationen finden Sie unter „Anhang – Bayes'scher Filter“ (Seite 294).

Die Bayes'sche Analyse ist standardmäßig **NICHT** aktiviert.

WICHTIG

Aktivieren Sie das Lernen anhand ausgehender E-Mails mindestens eine Woche lang, bevor Sie den Filter aktivieren. Dies ist erforderlich, da der Bayes'sche Filter erst durch die Anpassung an Ihre E-Mail-Muster eine maximale Erkennungsquote erzielen kann.

Konfigurieren des Bayes'schen Filters

Das Konfigurieren des Bayes'schen Filters erfolgt in zwei Phasen:

Phase 1: Lernphase des Bayes'schen Filters

Phase 2: Aktivierung des Bayes'schen Filters

Phase 1: Lernphase des Bayes'schen Filters

Der Bayes'sche Filter kann auf zwei Arten trainiert werden:

Methode 1: Automatisch durch ausgehende E-Mails.

GFI MailEssentials verarbeitet erwünschte E-Mails (Ham), indem ausgehende E-Mails gescannt werden. Der Bayes'sche Filter kann aktiviert werden, nachdem mindestens 500 ausgehende E-Mails (bei überwiegend englischsprachigen Nachrichten) bzw. 1000 ausgehende E-Mails (bei nicht englischsprachigen Nachrichten) erfasst worden sind.

Gehen Sie dazu wie folgt vor:

1. Wählen Sie **Anti-Spam > Anti-Spam-Filter > Bayes'sche Analyse** aus.

2. Wählen Sie **Ausgehende E-Mails automatisch analysieren** aus.

3. Klicken Sie auf **Übernehmen**.

Methode 2: Manuell mithilfe vorhandener E-Mails.

Kopieren Sie 500–1.000 E-Mails aus Ihren gesendeten Objekten in den Unterordner **Diese E-Mail ist**

kein Spam der öffentlichen **GFI Anti-Spam-Ordner**. Dies trainiert den Bayes'schen Filter auf dieselbe Weise wie die laufende Erfassung ausgehender E-Mails.

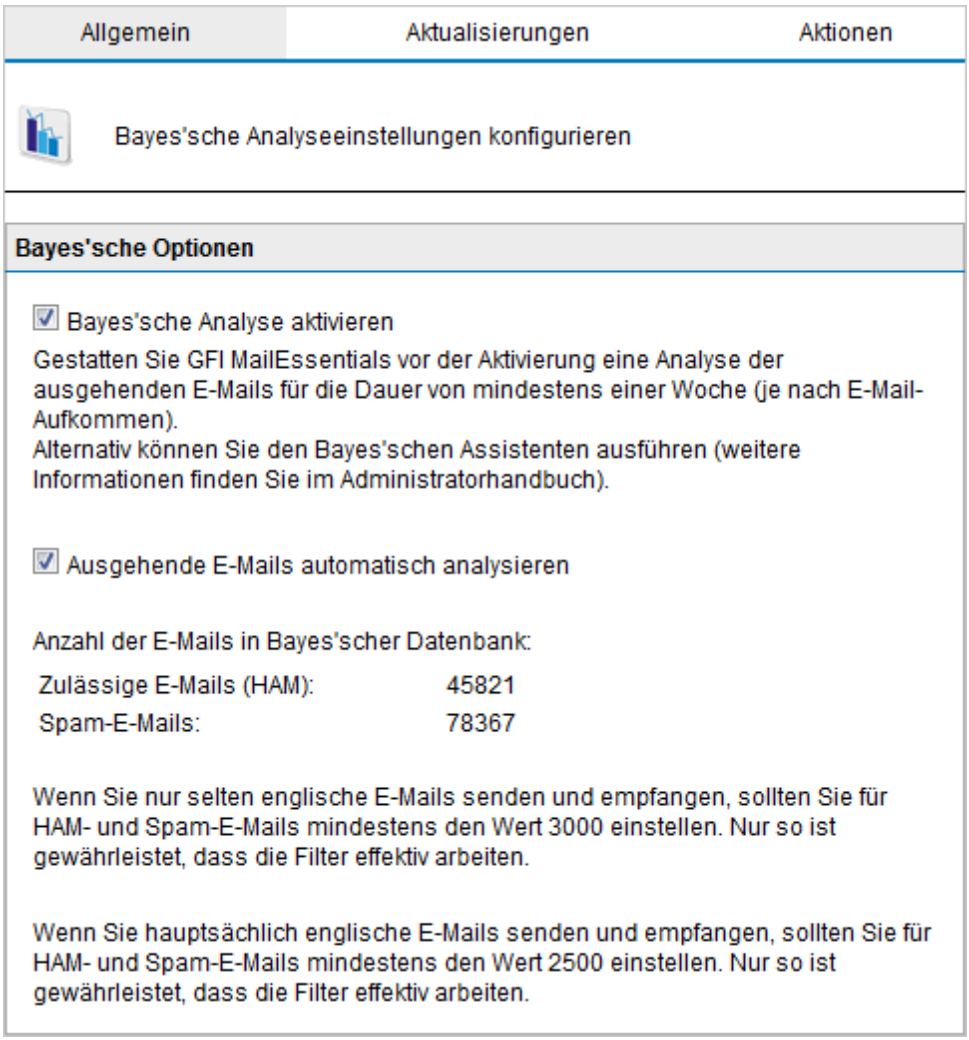
> **HINWEIS**
>
> Damit Sie diese Option verwenden können, muss das Scannen öffentlicher Ordner aktiviert sein. Weitere Informationen finden Sie unter „Scannen öffentlicher Ordner“ (Seite 174).

Phase 2: Aktivierung des Bayes'schen Filters

Nachdem der Bayes'sche Filter trainiert wurde, muss er aktiviert werden.

1. Wählen Sie in der Konfigurationskonsole von GFI MailEssentials die Optionen **Anti-Spam > Anti-Spam-Filter > Bayes'sche Analyse** aus.

2. Wählen Sie auf der Registerkarte **Allgemein** die Option **Bayes'sche Analyse aktivieren** aus.


Allgemein
Aktualisierungen
Aktionen
Bayes'sche Analyseeinstellungen konfigurieren
Bayes'sche Optionen
Bayes'sche Analyse aktivieren
Gestatten Sie GFI MailEssentials vor der Aktivierung eine Analyse der ausgehenden E-Mails für die Dauer von mindestens einer Woche (je nach E-Mail-Aufkommen).
Alternativ können Sie den Bayes'schen Assistenten ausführen (weitere Informationen finden Sie im Administratorhandbuch).
Ausgehende E-Mails automatisch analysieren
Anzahl der E-Mails in Bayes'scher Datenbank:
Zulässige E-Mails (HAM): 45821
Spam-E-Mails: 78367
Wenn Sie nur selten englische E-Mails senden und empfangen, sollten Sie für HAM- und Spam-E-Mails mindestens den Wert 3000 einstellen. Nur so ist gewährleistet, dass die Filter effektiv arbeiten.
Wenn Sie hauptsächlich englische E-Mails senden und empfangen, sollten Sie für HAM- und Spam-E-Mails mindestens den Wert 2500 einstellen. Nur so ist gewährleistet, dass die Filter effektiv arbeiten.

Screenshot 77: Eigenschaften der Bayes'schen Analyse

3. Konfigurieren Sie auf der Registerkarte **Aktualisierungen**, wie häufig die Spam-Datenbank aktualisiert werden soll, indem Sie **Automatisch auf Aktualisierungen prüfen** aktivieren und das Intervall in Stunden festlegen.

HINWEIS

Klicken Sie auf **Aktualisierungen jetzt herunterladen...**, um verfügbare Aktualisierungen sofort herunterzuladen.

HINWEIS

Sie können Aktualisierungen über einen Proxy-Server herunterladen. Weitere Informationen finden Sie unter „Proxy-Einstellungen“ (Seite 246).

4. Klicken Sie auf die Registerkarte **Aktionen**, um auszuwählen, was mit Nachrichten geschehen soll, die als Spam identifiziert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

5. Klicken Sie auf **Übernehmen**.

HINWEIS

GFI MailEssentials beinhaltet auch einen Assistenten für die Bayes'sche Analyse, mit dem Sie den Bayes'schen Filter auf einem anderen Computer trainieren können, auf dem GFI MailEssentials nicht installiert ist. Weitere Informationen finden Sie unter „Trainieren des Bayes'schen Analysefilters“ (Seite 295).

6.1.14 Whitelist

HINWEIS

Die Whitelist betrifft nur die Anti-Spam-Filter, nicht jedoch die E-Mail-Sicherheit oder die Inhaltsfilterung.

Die Whitelist enthält Listen von Kriterien, die zulässige E-Mails identifizieren. E-Mails, die diesen Kriterien entsprechen, werden nicht von Anti-Spam-Filtern geprüft und immer direkt dem Empfänger zugestellt. E-Mails können anhand folgender Kriterien auf die Whitelist gesetzt werden:

- E-Mail-Adresse, E-Mail-Domäne oder IP-Adresse des Absenders
- Absender, an die zuvor eine E-Mail gesendet wurde (Auto-Whitelist)
- Empfänger (lokale E-Mail-Adressen von der Filterung ausschließen)
- Stichwörter im E-Mail-Text oder im Betreff

Die Whitelist und Auto-Whitelist sind standardmäßig aktiviert.

Wichtige Hinweise

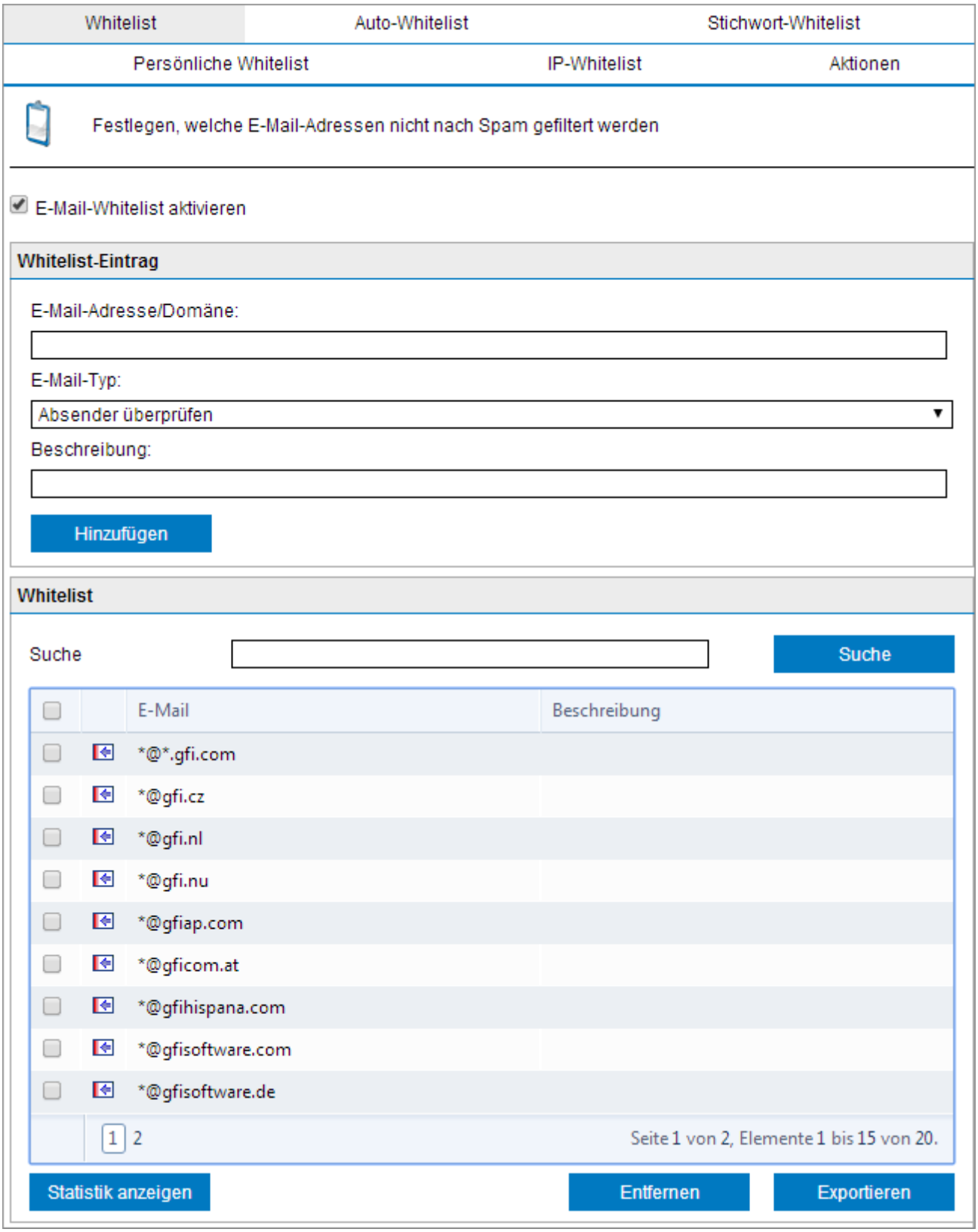
Das Verwenden der Auto-Whitelist wird dringend empfohlen, weil dadurch ein hoher Prozentsatz an falsch-positiven Ergebnissen eliminiert wird.

Fügen Sie zur Stichwort-Whitelist Begriffe hinzu, die von Spammern nicht verwendet werden und die sich auf Ihr Unternehmen beziehen, z. B. Produktnamen. Durch Eingabe zu vieler Stichwörter erhöht sich die Wahrscheinlichkeit, dass E-Mails nicht von GFI MailEssentials gefiltert und an die Benutzerpostfächer zugestellt werden.

Der Anti-Spoofing-Filter verfehlt seinen Zweck, wenn ein interner Benutzer auf die Whitelist gesetzt wird. Weitere Informationen finden Sie unter „Anti-Spoofing“ (Seite 131).

Konfigurieren der Whitelist

1. Wählen Sie **Anti-Spam > Whitelist** aus.



Screenshot 78: Registerkarte für die Whitelist

2. Legen Sie auf der Registerkarte **Whitelist** die E-Mail-Adressen und Domänen fest, die auf der Whitelist stehen sollen. Aktivieren/deaktivieren Sie die Option **E-Mail-Whitelist aktivieren**, um die Whitelist zu aktivieren/deaktivieren. Führen Sie folgende Schritte durch:

Aktion	Beschreibung
Whitelist-Eintrag hinzufügen	1. Geben Sie unter **E-Mail-Adresse/Domäne** eine E-Mail-Adresse oder Domäne ein, die der Whitelist hinzugefügt werden soll. **Beispiel:** . *@companysupport.com oder *@*.edu. 2. Geben Sie unter **E-Mail-Typ** den E-Mail-Header an, um die entsprechenden E-Mails der Whitelist hinzuzufügen. **HINWEIS** Weitere Informationen zum Unterschied zwischen SMTP und MIME finden Sie unter: http://go.gfi.com/?pageid=ME_DifferenceSMTPMIME 3. Im Feld **Beschreibung** können Sie eine Beschreibung hinzufügen (optional). 4. Klicken Sie auf **Hinzufügen**.
Whitelist-Einträge entfernen	1. Wählen Sie einen oder mehrere Einträge aus der **Whitelist** aus. 2. Klicken Sie auf **Entfernen**.
Whitelist-Eintrag suchen	1. Geben Sie unter **Suchen** Informationen zum gesuchten Whitelist-Eintrag ein. 2. Klicken Sie auf **Suchen**, um eine Liste übereinstimmender Begriffe anzuzeigen.
Statistik anzeigen	Mit der Schaltfläche **Statistik anzeigen** können Sie die Gesamtanzahl der blockierten E-Mails pro Whitelist-Eintrag anzeigen.
Whitelist-Einträge importieren	1. Geben Sie den vollständigen Pfad und Dateinamen für den Import der zuvor exportierten Daten an. 2. Klicken Sie auf **Importieren**, um die Einträge zu importieren.
Whitelist-Einträge exportieren	Klicken Sie auf **Exportieren**, um die aktuelle Liste von Whitelist-Einträgen in eine XML-Datei zu exportieren.

3. Wählen Sie die Registerkarte **Auto-Whitelist** aus, um folgende Optionen zu konfigurieren:

Option	Beschreibung
Auto-Whitelist automatisch erweitern:	Bei Auswahl dieser Option werden die Empfänger ausgehender E-Mails automatisch zur Auto-Whitelist hinzugefügt.
E-Mail-Auto-Whitelist aktivieren	Wählen Sie diese Option aus, um Auto-Whitelist zu aktivieren. Die Absender eingehender E-Mails werden mit der Auto-Whitelist abgeglichen. Ist ein Absender in der Liste vorhanden, wird die E-Mail direkt an das Postfach des Empfängers weitergeleitet.
Maximal zulässige Einträge für Auto-Whitelist:	Geben Sie an, wie viele Einträge die Auto-Whitelist maximal enthalten darf. Sobald dieses Limit überschritten wird, werden die ältesten und am wenigsten verwendeten Einträge automatisch durch neue Einträge ersetzt. **HINWEIS** Ein Wert, der größer als 30.000 ist, kann sich negativ auf die Leistung von GFI MailEssentials auswirken.

4. Geben Sie auf der Registerkarte **Stichwort-Whitelist** Stichwörter ein, die E-Mails als gültig kennzeichnen:

Option	Beschreibung
Whitelist der E-Mail-Textschlüsselwörter aktivieren	Wählen Sie diese Option aus, um den E-Mail-Text auf Stichwörter zu prüfen, die eine E-Mail als gültig kennzeichnen. Fügen Sie Ihre Stichwörter in der Liste **Stichwörter im Textkörper** hinzu. Sie können auch Stichwortlisten aus einer bzw. in eine XML-Datei importieren bzw. exportieren.

Option	Beschreibung
Whitelist für Schlüsselwörter im E-Mail-Betreff aktivieren	Wählen Sie diese Option aus, um den E-Mail-Betreff auf Stichwörter zu prüfen, die eine E-Mail als gültig kennzeichnen. Fügen Sie Ihre Stichwörter in der Liste **Betreffstichwörter** hinzu. Sie können auch Stichwortlisten aus einer bzw. in eine XML-Datei importieren bzw. exportieren.
Nur ganze Wörter berücksichtigen (Wörter/Wortgruppen im Betreff/Textkörper)	Wenn Sie diese Option auswählen, werden nur ganze Wörter aus der Stichwort-Whitelist abgeglichen, um eine E-Mail als gültig zu identifizieren.

5. Konfigurieren Sie auf der Registerkarte **IP-Whitelist** die folgenden Optionen:

Option	Beschreibung
IP-Whitelist aktivieren	Wählen Sie diese Option aus, um E-Mails von bestimmten IP-Adressen in die Whitelist aufzunehmen.
IP-Whitelist-Einträge hinzufügen	1. Geben Sie Folgendes an: » **Einzelner Computer/CIDR**: Geben Sie eine einzelne IP-Adresse oder einen Bereich von IP-Adressen in der CIDR-Notation ein. » **Gruppe von Computern**: Geben Sie die **Subnetzadresse** und die **Subnetzmaske** der Gruppe von IP-Adressen an, die der Whitelist hinzugefügt werden soll. 2. Geben Sie eine **Beschreibung** ein (optional). 3. Klicken Sie auf **Hinzufügen**.
IP-Whitelist-Einträge entfernen	Wählen Sie die zu entfernenden IP-Adressen aus, und klicken Sie auf **Entfernen**.

6. Klicken Sie auf die Registerkarte **Aktionen**, um die Protokollierung von Whitelist-Ereignissen in einer Datei zu aktivieren/deaktivieren. Geben Sie den Pfad/Ordner an, unter dem die generierte Protokolldatei gespeichert werden soll.

7. Klicken Sie auf **Übernehmen**.

Persönliche Whitelist

Die persönliche Whitelist ist eine zusätzliche Whitelist als Ergänzung der globalen Whitelist. Sie ist standardmäßig deaktivert und kann zur Aktivierung durch die Benutzer freigeschaltet werden, die dann einer persönlichen, von ihnen verwalteten Whiteliste spezifische E-Mail-Adressen hinzufügen können. Weitere Informationen finden Sie unter „Endbenutzeraktionen“ (Seite 19).

Zu Verwaltungszwecken kann der Administrator auch spezifische E-Mail-Adressen entfernen, die die Benutzer zur persönlichen Whitelist hinzugefügt haben.

Aktivieren/Deaktivieren der persönlichen Whitelist

1. Wählen Sie **Anti-Spam > Whitelist** aus.

Screenshot 79: Persönliche Whitelist

2. Wählen Sie die Registerkarte **Persönliche BWhitelist** aus und aktivieren oder deaktivieren Sie die Option **Persönliche E-Mail-Whitelist aktivieren**, um die persönliche Whitelist freizuschalten bzw. zu sperren.

3. Klicken Sie auf **Übernehmen**.

Entfernen von E-Mails der persönlichen Whitelist

1. Wählen Sie **Anti-Spam > Whitelist** aus und zeigen Sie dann die Registerkarte **Persönliche Whitelist** an.

2. Wählen Sie aus dem Listenfeld **Benutzer** dann den Benutzer aus, für den eine E-Mail-Adresse gelöscht werden soll.

3. Wählen Sie von der Adressliste eine E-Mail-Adresse aus. Klicken Sie auf **Entfernen**.

4. Klicken Sie auf **Übernehmen**.

6.1.15 Neue Absender

Der Filter für neue Absender identifiziert E-Mails von Absendern, an die bislang keine E-Mails gesendet wurden. Diese Absender werden als neue Absender klassifiziert, nachdem ein Abgleich mit den in den Whitelists gespeicherten Adressen durchgeführt worden ist.

Der Filter für neue Absender identifiziert nur E-Mails, die keine Spam-typischen Merkmale aufweisen und deren Absender in keiner Whitelist verzeichnet sind.

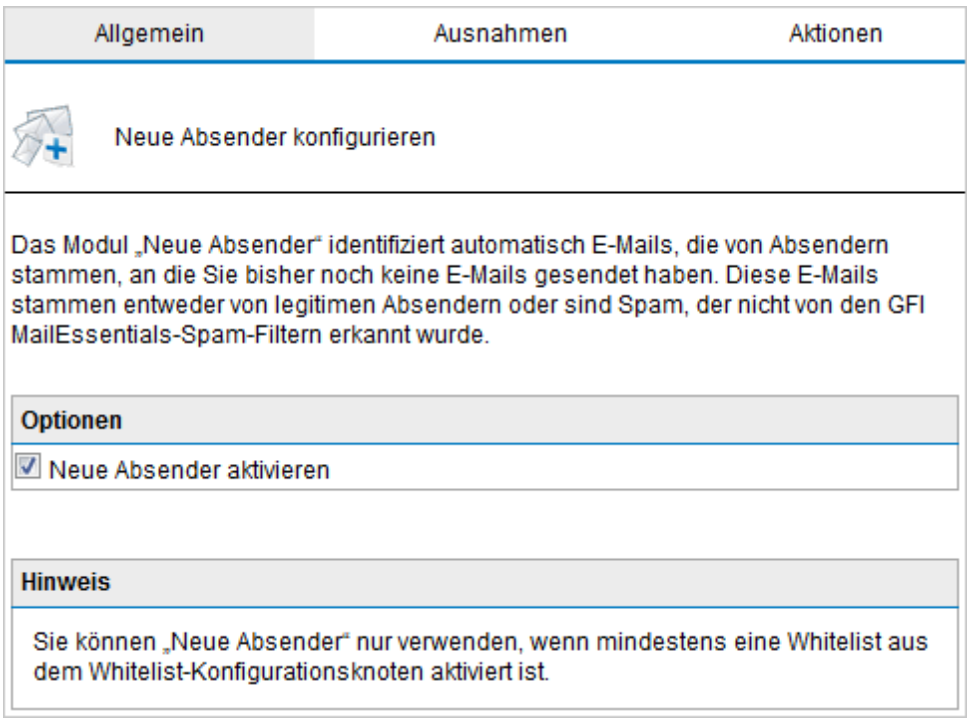
Dieser Filter ist **NICHT** standardmäßig aktiviert.

Wichtig

Um die Funktion Neue Absender nutzen zu können, muss mindestens eine der verfügbaren Whitelists aktiviert sein. Bei deaktivierten Whitelist-Funktionen (und einer ungehinderten Filterung durch die anderen Spam-Filter) werden alle eingehenden Nachrichten an den Posteingang des Empfängers zugestellt. In den Ordner für neue Absender werden **NUR** E-Mails verschoben, die keine Spam-typischen Merkmale aufweisen und deren Absender in keiner Whitelist verzeichnet sind.

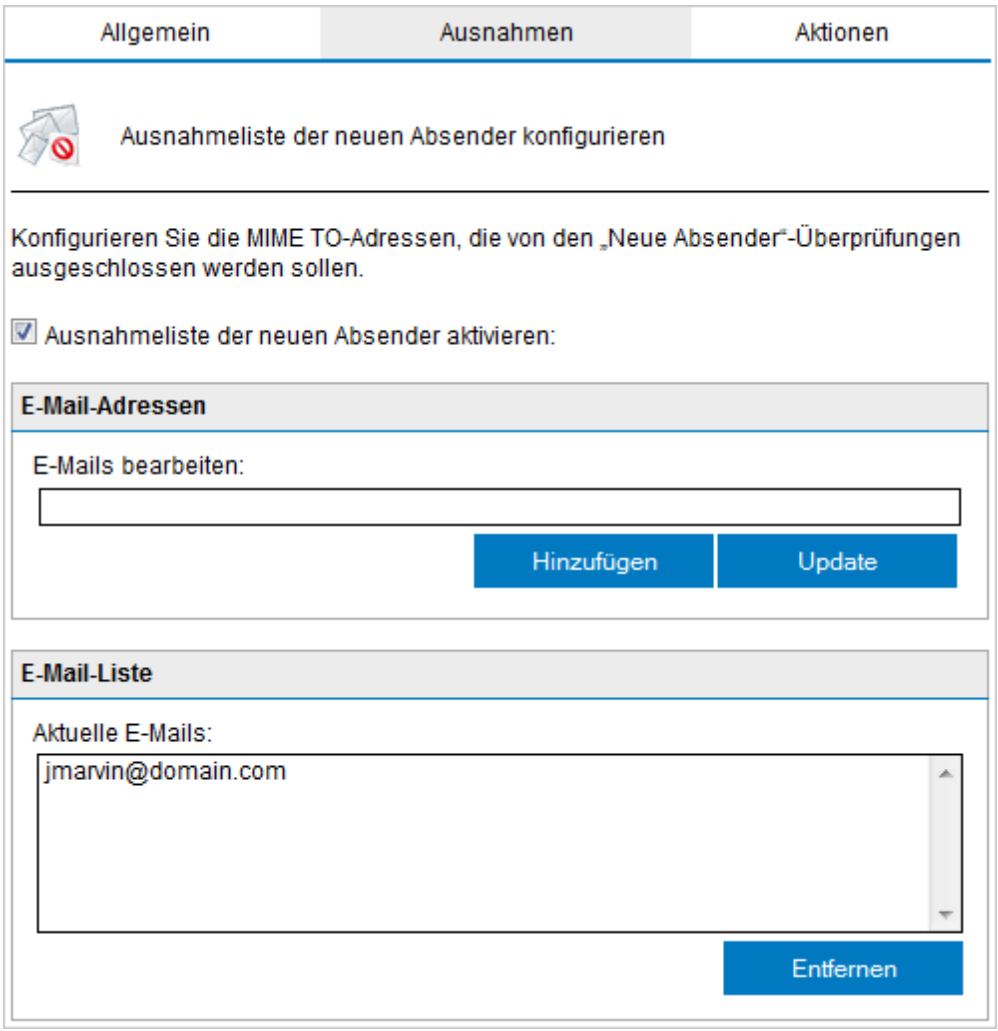
Konfigurieren des Filters für neue Absender

1. Wählen Sie **Anti-Spam > Neue Absender** aus.


Allgemein
Ausnahmen
Aktionen
Neue Absender konfigurieren
Das Modul „Neue Absender" identifiziert automatisch E-Mails, die von Absendern stammen, an die Sie bisher noch keine E-Mails gesendet haben. Diese E-Mails stammen entweder von legitimen Absendern oder sind Spam, der nicht von den GFI MailEssentials-Spam-Filtern erkannt wurde.
Optionen
Neue Absender aktivieren
Hinweis
Sie können „Neue Absender" nur verwenden, wenn mindestens eine Whitelist aus dem Whitelist-Konfigurationsknoten aktiviert ist.

Screenshot 80: Neue Absender - Allgemein

2. Wählen Sie auf der Registerkarte **Allgemein** die Option **Neue Absender aktivieren** aus, um die Prüfung auf neue Absender für alle eingehenden Nachrichten zu aktivieren.



Screenshot 81: Neue Absender - Ausnahmen

3. Konfigurieren Sie auf der Registerkarte **Ausnahmen** die Absender und Empfänger, deren E-Mails von der Prüfung auf neue Absender ausgeschlossen werden sollen.

Option	Beschreibung
Ausnahmeliste der neuen Absender aktivieren	Wählen Sie diese Option aus, um die Liste der Ausnahmen zu aktivieren.
Ausnahme hinzufügen	Geben Sie eine auszuschließende E-Mail-Adresse ein, und klicken Sie auf **Hinzufügen**. Wiederholen Sie dies für jede Adresse, die Sie hinzufügen möchten.
Ausnahme bearbeiten	1. Wählen Sie in der **E-Mail-Liste** eine Ausnahme aus. 2. Bearbeiten Sie die E-Mail-Adresse. 3. Klicken Sie auf **Aktualisieren**.
Ausnahme löschen	Wählen Sie in der **E-Mail-Liste** eine Ausnahme aus, und klicken Sie auf **Entfernen**.

4. Klicken Sie auf die Registerkarte **Aktionen**, um auszuwählen, was mit Nachrichten geschehen soll, die als Spam identifiziert werden. Weitere Informationen finden Sie unter „Spam-Aktionen - Umgang mit Spam-E-Mails“ (Seite 150).

5. Klicken Sie auf **Übernehmen**.

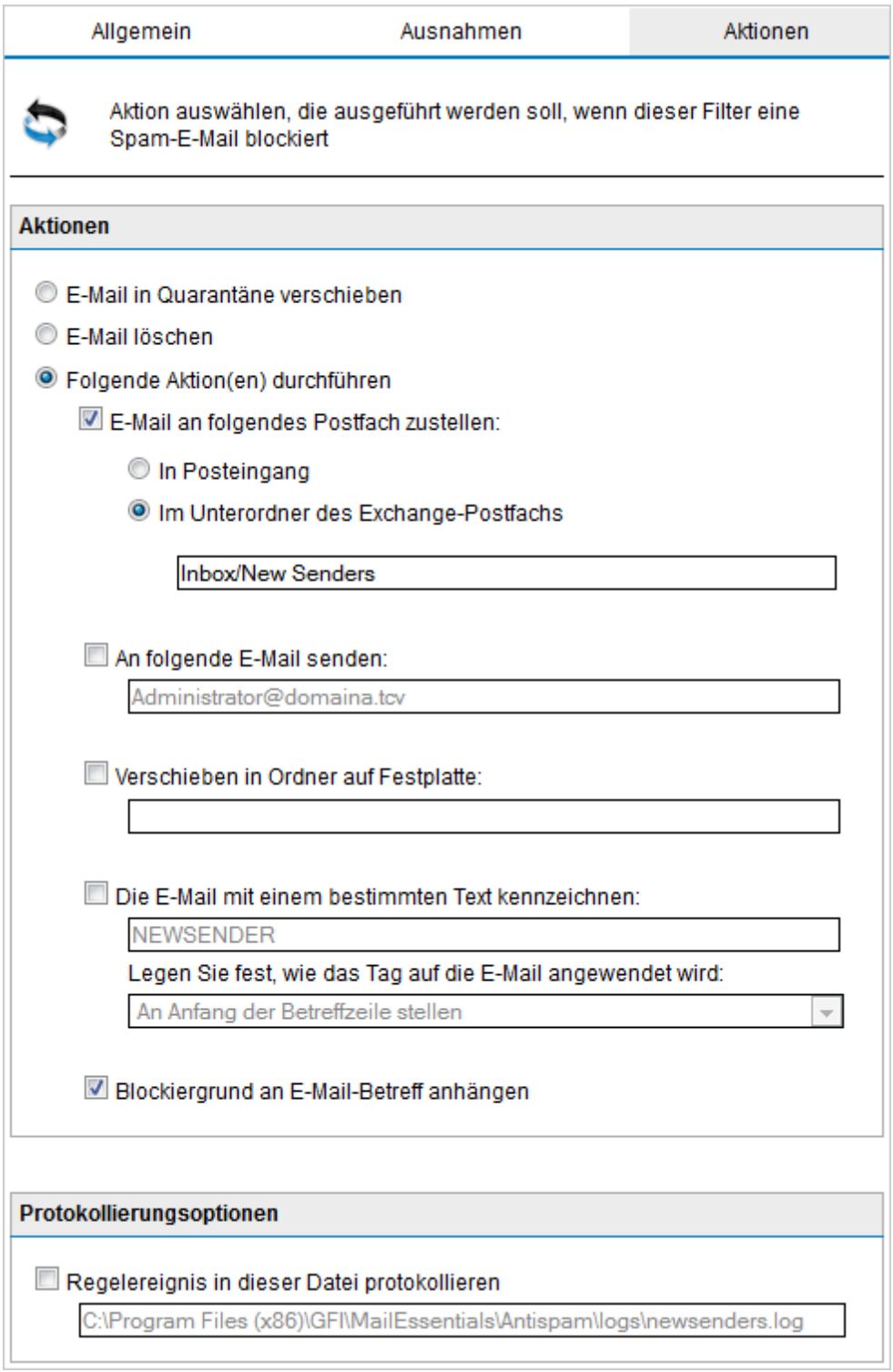
6.2 Spam-Aktionen – Umgang mit Spam-E-Mails

Auf der Registerkarte **Aktionen** in den Anti-Spam-Filtereigenschaften wird definiert, was mit als Spam klassifizierten E-Mails geschehen soll. Sie können für jeden Spam-Filter verschiedene Aktionen definieren.

» **Beispiel**: E-Mails, die vom SpamRazer-Filter erkannt werden, sollen gelöscht werden, aber E-Mails, die vom E-Mail-Blocklist-Filter als Spam klassifiziert werden, sollen nicht gelöscht werden.

6.2.1 Konfigurieren von Spam-Aktionen

Wählen Sie auf der Registerkarte **Aktionen** eine Option aus, um zu definieren, was mit E-Mails geschehen soll, die als Spam gekennzeichnet werden.



Screenshot 82: Anti-Spam-Aktionen

Aktion	Beschreibung
E-Mail in Quarantäne verschieben	Als Spam erkannte E-Mails werden im Quarantänespeicher abgespeichert. Die anderen Spam-Aktionen sind deaktiviert, wenn die E-Mail in Quarantäne verschoben wird. Weitere Informationen finden Sie unter „Quarantäne“ (Seite 208).
E-Mail löschen	E-Mails, die von diesem Spam-Filter blockiert werden, sollen gelöscht werden. Die anderen Spam-Aktionen sind deaktiviert, wenn die E-Mail gelöscht wird.

Aktion	Beschreibung
E-Mail an folgendes Postfach zustellen	Wählen Sie den Ordner aus, in den die E-Mail zugestellt werden soll. Folgende Optionen sind verfügbar: » **In Posteingang** - Leitet Spam an den Posteingang des Benutzers weiter. » **In Exchange Junk-Mail-Ordner** - Leitet Spam an den Junk-Mail-Ordner des Benutzers weiter. Diese Option funktioniert nur, wenn GFI MailEssentials auf dem Microsoft Exchange-Server installiert ist. Sie ist nur für den Filter „Neue Absender“ verfügbar. » **Im Unterordner des Exchange-Postfachs** - Leitet alle Spam-Nachrichten an einen bestimmten Ordner im Postfach des Benutzers weiter. Geben Sie den Ordner ein, in den Spam-E-Mails verschoben werden sollen. • **Beispiel 1:** Geben Sie `Spam-verdächtig` ein, um einen benutzerdefinierten Ordner auf der Ebene des Posteingangsordners zu erstellen. • **Beispiel 2:** Geben Sie `Posteingang\Spam-verdächtig` ein, um einen benutzerdefinierten Ordner innerhalb des Posteingangsordners zu erstellen. **HINWEIS:** Voraussetzungen für diese Option: • GFI MailEssentials ist auf dem Microsoft® Exchange-Server installiert. Ist GFI MailEssentials nicht auf dem Microsoft® Exchange-Server installiert. Konfigurieren Sie den E-Mail-Server so, dass E-Mails weitergeleitet werden, oder verwenden Sie den Regel-Manager. Weitere Informationen finden Sie unter „Verschieben von Spam-E-Mails in Benutzerpostfachordner“ (Seite 266). • Der E-Mail-Server ist Microsoft® Exchange Server 2003 oder Microsoft® Exchange Server 2007/2010 und hat die Postfachserverrolle. Bei Microsoft® Exchange 2010 ist ein dediziertes Benutzerkonto erforderlich, um diese Option zu aktivieren. Weitere Informationen finden Sie unter „Verschieben von Spam in einen Exchange 2010-Ordner“ (Seite 268).
An folgende E-Mail senden	Identifizierte Spam-E-Mails werden an eine bestimmte E-Mail-Adresse gesendet. **Beispiel:** Alle Spam-E-Mails werden an eine E-Mail-Adresse weitergeleitet, wo überprüft wird, ob E-Mails fälschlicherweise als Spam markiert wurden. Die Betreffzeile der E-Mail hat folgendes Format: `[Empfänger] [Betreff]`
Verschieben in Ordner auf Festplatte	Identifizierte Spam-E-Mails werden unter dem angegebenen Pfad gespeichert. **Beispiel:** `C:\Spam\` Die Dateinamen der gespeicherten E-Mails haben folgendes Format: `[Absender_Empfänger_Betreff_Nummer_.eml]` **Beispiel:**`C:\Spam\jim@comp.com_bob@comp.com_MailOffers_1_.eml`)

Aktion	Beschreibung
Die E-Mail mit einem bestimmten Text kennzeichnen	Wählen Sie diese Option aus, um dem E-Mail-Betreff eine Kennzeichnung hinzuzufügen. Geben Sie den Text ein, der als Kennzeichnung verwendet werden soll, und geben Sie an, wo er eingefügt werden soll: » **An Anfang der Betreffzeile stellen** - Die Kennzeichnung wird zu Beginn des E-Mail-Betreffs eingefügt (als Präfix). **Beispiel:** `[SPAM]Free Web Mail` » **An Betreffzeile anhängen** - Die Kennzeichnung wird am Ende des E-Mail-Betreffs eingefügt (als Suffix). **Beispiel:** `Free Web Mail[SPAM]` » **Tag in einen X-Header einfügen...** - Die gewünschte Kennzeichnung wird der E-Mail als neuer X-Header hinzugefügt. Der X-Header hat dabei folgendes Format: • `X-GFIME-SPAM: [Text der Kennzeichnung]` • `X-GFIME-SPAM-REASON: [Begründung]` **Beispiel:** – `X-GFIME-SPAM: [SPAM]` – `X-GFIME-SPAM-REASON: [Prüfung durch IP-DNS-Blocklist fehlgeschlagen – Gesendet von Blocklist-Domäne]` **HINWEIS** Der Regel-Manager kann zum Verschieben von E-Mails verwendet werden, wenn diese Funktion genutzt wird.
Blockiergrund an E-Mail-Betreff anhängen	Ist diese Option aktiviert, werden der Name des Filters, der die E-Mail blockiert hat, und die Begründung für das Blockieren zum Betreff der blockierten E-Mail hinzugefügt.
Regelereignis in dieser Datei protokollieren	Die Identifizierung einer Spam-E-Mail wird in einer Protokolldatei Ihrer Wahl protokolliert. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert: *<GFI MailEssentials Installationspfad>*`\GFI\MailEssentials\AntiSpam\Logs\<<filtername>.log` **HINWEIS** Protokolldateien können sehr groß werden. GFI MailEssentials bietet einen Protokollrotator, durch den in regelmäßigen Abständen oder bei Erreichen einer bestimmten Größe eine neue Protokolldatei erstellt wird. Um den Protokollrotator zu aktivieren, öffnen Sie **Anti-Spam > Anti-Spam-Einstellungen**. Aktivieren Sie auf der Registerkarte **Anti-Spam-Protokollierung** die Option **Protokollrotator aktivieren**. Legen Sie die Rotationsbedingung nach Zeit oder Dateigröße fest.

6.3 Sortieren der Anti-Spam-Filter nach Priorität

In GFI MailEssentials können Sie die Reihenfolge ändern, in der Anti-Spam-Prüfungen auf eingehende Nachrichten angewendet werden.

HINWEIS

Sie können die Reihenfolge aller verfügbaren Filter anpassen, mit Ausnahme des Filters **Neue Absender**, der automatisch mit der niedrigsten Priorität belegt wird. Dies liegt daran, dass er von den Ergebnissen der Whitelist-Prüfung und der anderen Anti-Spam-Filter abhängig ist.

In den meisten Fällen empfiehlt es sich, die Standardreihenfolge beizubehalten.

1. Wählen Sie **Anti-Spam > Filterpriorität** aus.

Screenshot 83: Zuweisen von Filterprioritäten

2. Wählen Sie einen Filter aus, und klicken Sie auf ↑ (nach oben), um ihm eine höhere Priorität zuzuweisen, oder auf ↓ (nach unten), um ihm eine niedrigere Priorität zuzuweisen.

> **HINWEIS**
>
> Durch Klicken auf **Standardeinstellungen** können Sie die Standardreihenfolge der Filter wiederherstellen.

3. Klicken Sie auf **Übernehmen**.

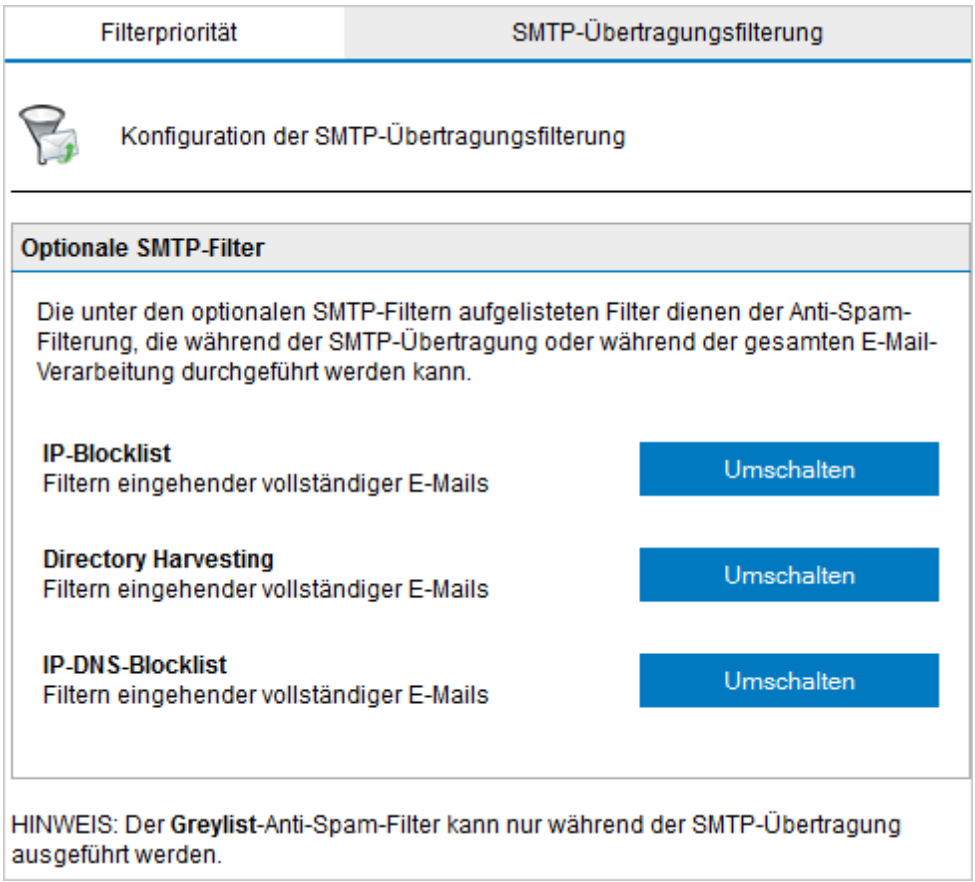
6.4 SMTP-Übertragungsfilterung

In GFI MailEssentials können Anti-Spam-Filter so konfiguriert werden, dass sie entweder beim Empfang der vollständigen E-Mail ausgeführt wird, oder dass sie eingehende E-Mails auf SMTP-Ebene filtern. Bei der SMTP-Übertragungsfilterung werden E-Mails gescannt, wenn sie empfangen werden.

Bei der Filterung auf SMTP-Ebene wird die Verbindung zur E-Mail getrennt und somit das Herunterladen der vollständigen E-Mail gestoppt. Dies spart Bandbreite und Verarbeitungsressourcen. Die Verbindung wird in diesem Fall sofort getrennt, und die E-Mail muss keine weiteren Anti-Spam-Filter durchlaufen.

> **WICHTIG**
>
> Verwenden Sie die SMTP-Übertragungsfilterung für eine bestmögliche Nutzung, wenn GFI MailEssentials auf einem Internet-Gateway installiert ist, oder wenn es der erste Server ist, der E-Mails aus dem Internet empfängt.

1. Öffnen Sie **Anti-Spam > Filterpriorität**, und wählen Sie die Registerkarte **SMTP-Übertragungsfilterung** aus.



Screenshot 84: Eigenschaften der SMTP-Übertragungsfilterung

2. Klicken Sie auf **Wechseln**, um das Directory Harvesting zwischen folgenden beiden Optionen umzuschalten:

Option	Beschreibung
Filtern eingehender vollständiger E-Mails	Die Filterung erfolgt nach dem Empfang der vollständigen E-Mail.
Filtern während der SMTP-Übertragung	Die Filterung erfolgt während der SMTP-Übertragung. Bei Auswahl dieser Option wird der Filter immer vor allen anderen Spam-Filtern ausgeführt.

> **HINWEIS**
>
> Der Greylist-Filter wird nur auf der SMTP-Übertragungsebene ausgeführt.

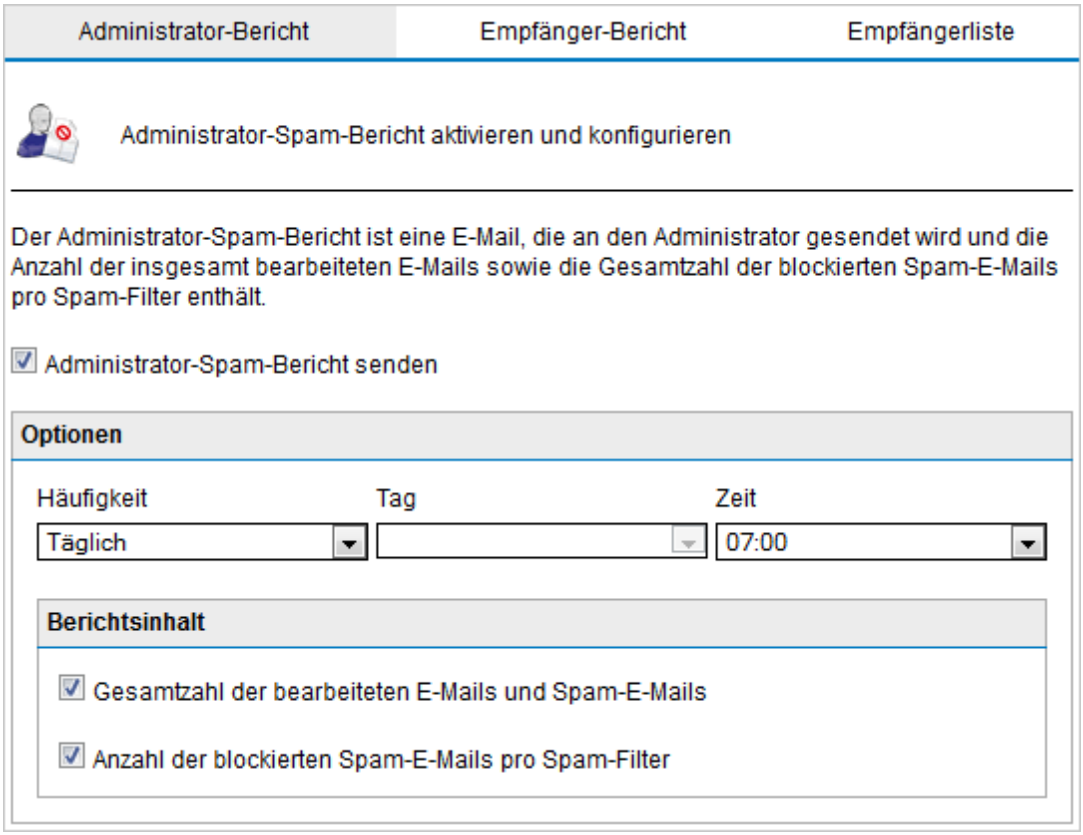
3. Klicken Sie auf **Übernehmen**.

6.5 Spam-Bericht

Der Spam-Bericht enthält einen kurzen Bericht und wird per E-Mail an einen Administrator oder Benutzer gesendet. In diesem Bericht sind die Gesamtzahl der E-Mails enthalten, die von GFI MailEssentials verarbeitet wurden, sowie die Gesamtzahl der in einem bestimmten Zeitraum blockierten Spam-E-Mails (seit dem letzten Spam-Bericht).

6.5.1 Konfigurieren von Spam-Berichten – Administrator-Spam-Bericht

1. Wählen Sie **Anti-Spam > Spam-Bericht**.



Screenshot 85: Eigenschaften des Administrator-Spam-Berichts

2. Aktivieren Sie auf der Registerkarte **Administrator-Bericht** die Option **Administrator-Spam-Bericht senden**, um den Spam-Bericht zu aktivieren.

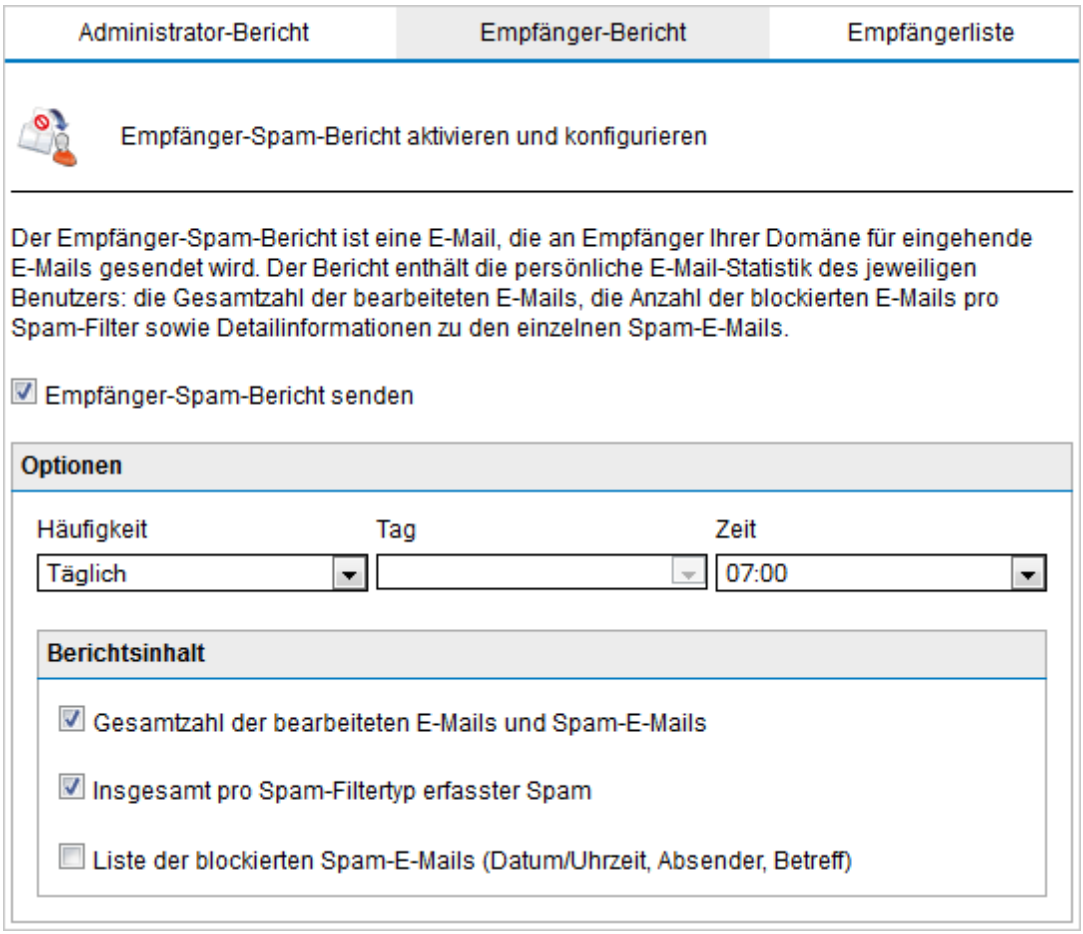
3. Konfigurieren Sie die Häufigkeit des E-Mail-Versands (Täglich, Wöchentlich, Monatlich), und geben Sie ein Datum und eine Uhrzeit für den Versand ein.

4. Geben Sie den Berichtsinhalt an, der per E-Mail gesendet werden soll. Wählen Sie **Gesamtzahl der bearbeiteten E-Mails und Spam-E-Mails** oder **Anzahl der blockierten Spam-E-Mails pro Spam-Filter** oder beide Optionen aus.

5. Klicken Sie auf **Übernehmen**, um die Einstellungen abzuschließen.

6.5.2 Konfigurieren von Spam-Berichten – Empfänger-Spam-Bericht

1. Wählen Sie **Anti-Spam > Spam-Bericht**.


Administrator-Bericht
Empfänger-Bericht
Empfängerliste
Empfänger-Spam-Bericht aktivieren und konfigurieren
Der Empfänger-Spam-Bericht ist eine E-Mail, die an Empfänger Ihrer Domäne für eingehende E-Mails gesendet wird. Der Bericht enthält die persönliche E-Mail-Statistik des jeweiligen Benutzers: die Gesamtzahl der bearbeiteten E-Mails, die Anzahl der blockierten E-Mails pro Spam-Filter sowie Detailinformationen zu den einzelnen Spam-E-Mails.
Empfänger-Spam-Bericht senden
Optionen
Häufigkeit
Tag
Zeit
Täglich
07:00
Berichtsinhalt
Gesamtzahl der bearbeiteten E-Mails und Spam-E-Mails
Insgesamt pro Spam-Filtertyp erfasster Spam
Liste der blockierten Spam-E-Mails (Datum/Uhrzeit, Absender, Betreff)

Screenshot 86: Empfänger-Spam-Bericht

2. Aktivieren Sie auf der Registerkarte **Empfänger-Bericht** die Option **Empfänger-Spam-Bericht senden**, um den Spam-Bericht zu aktivieren.

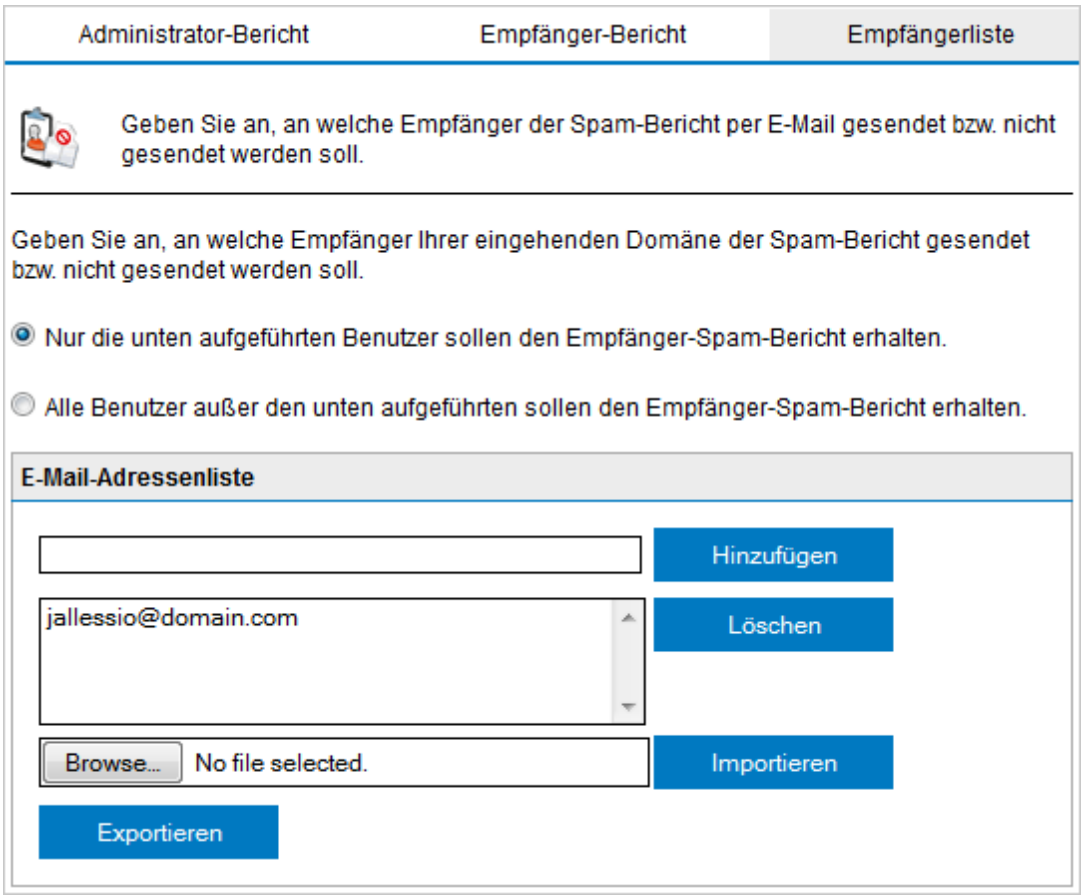
3. Konfigurieren Sie die Häufigkeit des E-Mail-Versands (Täglich, Wöchentlich, Monatlich), und geben Sie ein Datum und eine Uhrzeit für den Versand ein.

4. Geben Sie den Berichtsinhalt an, der per E-Mail gesendet werden soll:

» Gesamtzahl der bearbeiteten E-Mails und Spam-E-Mails

» Insgesamt erkannter Spam pro Spam-Filtertyp

» Liste der blockierten Spam-E-Mails oder eine Kombination aus den gewünschten Optionen


Administrator-Bericht
Empfänger-Bericht
Empfängerliste
Geben Sie an, an welche Empfänger der Spam-Bericht per E-Mail gesendet bzw. nicht gesendet werden soll.
Geben Sie an, an welche Empfänger Ihrer eingehenden Domäne der Spam-Bericht gesendet bzw. nicht gesendet werden soll.
Nur die unten aufgeführten Benutzer sollen den Empfänger-Spam-Bericht erhalten.
Alle Benutzer außer den unten aufgeführten sollen den Empfänger-Spam-Bericht erhalten.
E-Mail-Adressenliste
Hinzufügen
jallessio@domain.com
Löschen
Browse...
No file selected.
Importieren
Exportieren

Screenshot 87: Empfängerliste für Spam-Berichte

4. Wählen Sie die Registerkarte **Empfängerliste** aus, und fügen Sie die Benutzer hinzu, die einen Spam-Bericht erhalten sollen. Wählen Sie außerdem die Methode aus, anhand derer die Empfänger von Spam-Berichten bestimmt werden sollen.

Folgende Optionen sind verfügbar:

» Nur die unten aufgeführten Benutzer sollen den Empfänger-Spam-Bericht erhalten.

» Alle Benutzer außer den unten aufgeführten sollen den Empfänger-Spam-Bericht erhalten.

> **HINWEIS**
>
> Die Benutzerliste kann auch als XML-Datei importiert werden. Die Datei muss dieselbe Struktur wie von GFI MailEssentials exportierte Dateien aufweisen.

6. Klicken Sie auf **Übernehmen**, um die Einstellungen abzuschließen.

6.6 Anti-Spam-Einstellungen

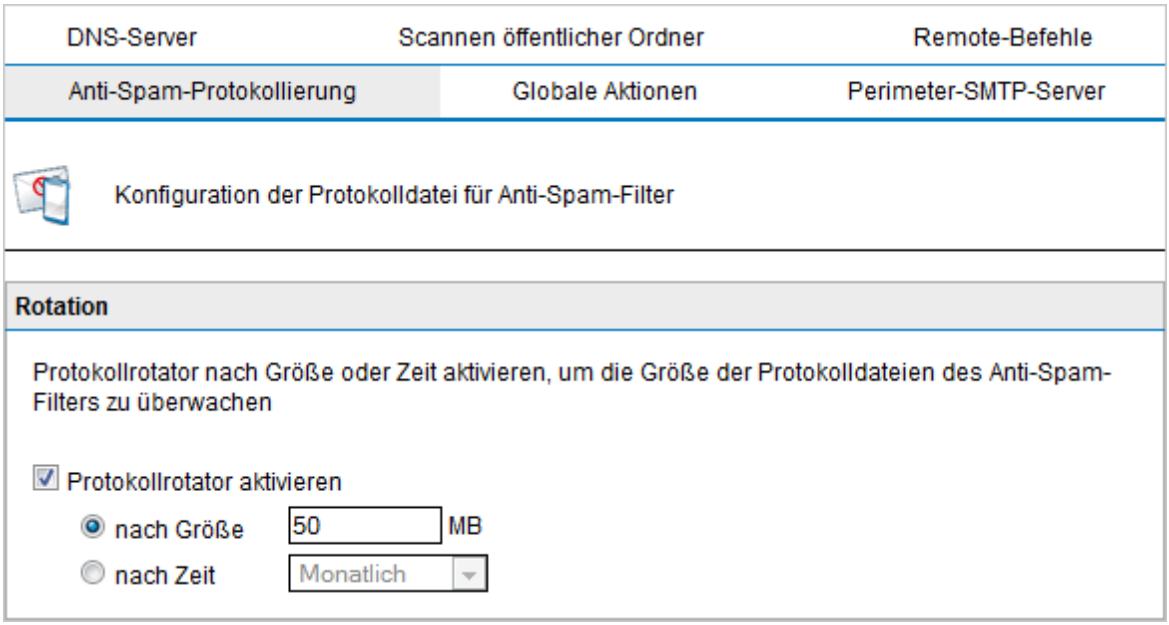
Die folgenden Einstellungen gelten nur für Anti-Spam-Filter und E-Mails, die durch Anti-Spam-Filter blockiert werden.

6.6.1 Protokollrotator

Protokolldateien können mit der Zeit sehr groß werden. GFI MailEssentials bietet einen Protokollrotator, durch den in regelmäßigen Abständen oder bei Erreichen einer bestimmten Größe eine neue Protokolldatei erstellt wird.

So aktivieren Sie den Protokollrotator:

1. Wählen Sie **Anti-Spam > Anti-Spam-Einstellungen** aus.



Screenshot 88: Protokollrotator

2. Aktivieren Sie auf der Registerkarte **Anti-Spam-Protokollierung** die Option **Protokollrotator aktivieren**, und legen Sie die Rotationsbedingung fest (**nach Größe** oder **nach Zeit**).

3. Geben Sie den Größen- oder Zeitwert ein, und klicken Sie auf **Übernehmen**.

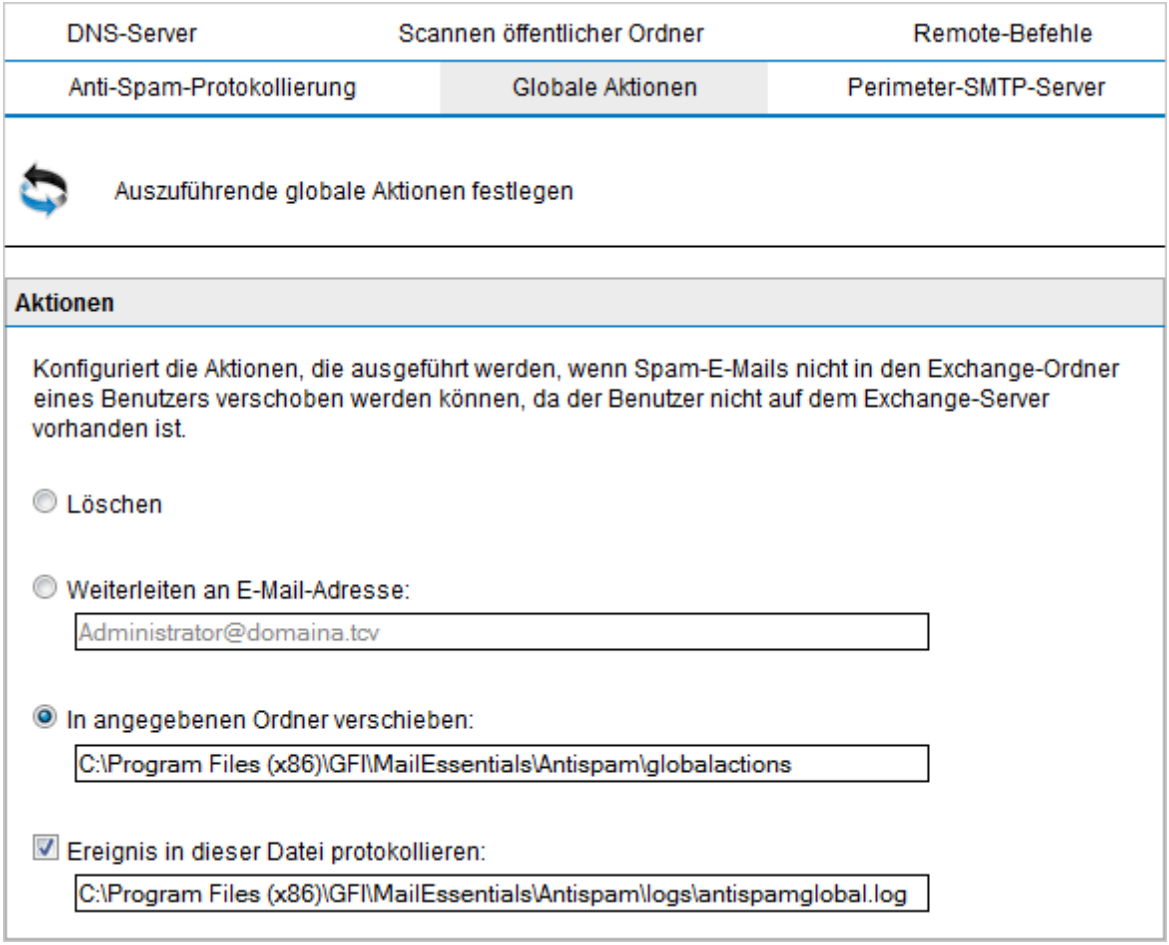
6.6.2 Globale Anti-Spam-Aktionen

Viele Spam-Mitteilungen werden an E-Mail-Adressen verschickt, die nicht mehr existieren. Diese E-Mails werden normalerweise einfach gelöscht. Aus Gründen der Fehlerbehebung oder zu Testzwecken können Sie diese E-Mails jedoch auch in einen Ordner verschieben oder an eine bestimmte E-Mail-Adresse weiterleiten.

> **HINWEIS**
>
> Dieser Abschnitt gilt nur für Installationen auf Microsoft® Exchange Server, bei denen die Spam-Aktion **In Unterordner des Benutzerpostfachs verschieben** aktiviert ist. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).
>
> Auf anderen Mailservern ist die Registerkarte für globale Anti-Spam-Aktionen nicht verfügbar.

Konfigurieren der globalen Anti-Spam-Aktionen

1. Wählen Sie **Anti-Spam > Anti-Spam-Einstellungen** aus.



Screenshot 89: Globale Aktionen

2. Wählen Sie auf der Registerkarte **Globale Aktionen** eine der folgenden Optionen aus:

» E-Mail löschen

» An eine E-Mail-Adresse weiterleiten

» In einen bestimmten Ordner verschieben

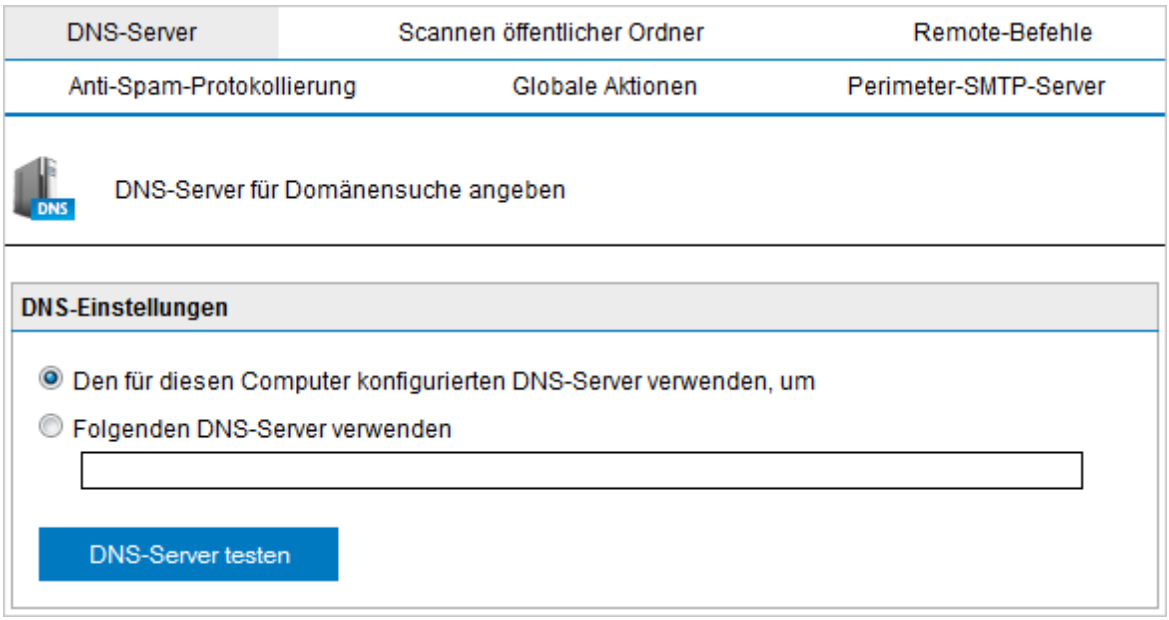
3. Um diese Ereignisse in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus.

4. Klicken Sie auf **Übernehmen**.

6.6.3 DNS-Servereinstellungen

DNS-Servereinstellungen sind in GFI MailEssentials sehr wichtig, da Anti-Spam-Filter wie die IP-DNS-Blocklist, die URI-DNS-Blocklist und SpamRazer bei der Spam-Filterung eine Domänensuche durchführen.

1. Wählen Sie in GFI MailEssentials Configuration die Optionen **Anti-Spam > Anti-Spam-Einstellungen** aus.



Screenshot 90: DNS-Servereinstellungen

1. Konfigurieren Sie auf der Registerkarte **DNS-Server** folgende Optionen:

Option	Beschreibung
Den für diesen Computer konfigurierten DNS-Server verwenden, um	Wählen Sie diese Option aus, um denselben DNS-Server wie das Betriebssystem zu verwenden, unter dem GFI MailEssentials installiert ist.
Folgenden DNS-Server verwenden	Wählen Sie diese Option aus, um einen DNS-Server festzulegen, der sich vom Server des lokalen Computers unterscheidet.

2. Klicken Sie auf **DNS-Server testen**, um die Verbindung mit dem festgelegten DNS-Server zu testen. Falls der Test nicht erfolgreich ist, geben Sie einen anderen DNS-Server an.

3. Klicken Sie auf **Übernehmen**.

6.6.4 Remote-Befehle

Mithilfe von Remote-Befehlen können Domänen oder Adressen der E-Mail-Blocklist/Whitelist für E-Mails hinzugefügt werden, und der Bayes'schen Filter kann mit Spam oder Ham (gültigen E-Mails) aktualisiert werden.

Remote-Befehle werden verwendet, indem sie per E-Mail an GFI MailEssentials geschickt werden. Wenn Sie eine E-Mail an **rcommands@mailessentials.com** (konfigurierbar) schicken, erkennt GFI MailEssentials, dass die Nachricht Remote-Befehle enthält. Diese werden dann wie unten beschrieben verarbeitet.

Remote-Befehle können für folgende Aufgaben verwendet werden:

1. Spam oder Ham zur Datenbank für die Bayes'sche Analyse hinzufügen

2. Stichwörter zur Stichwortprüfung für die Betreffzeile oder den Textkörper hinzufügen

3. Neue Adressen zum E-Mail-Blocklist-Filter und zur Whitelist hinzufügen

Konfigurieren von Remote-Befehlen

1. Klicken Sie auf **Anti-Spam > Anti-Spam-Einstellungen** und wählen Sie auf der Registerkarte **Remote-Befehle** die Option **Remote-Befehle aktivieren** aus.

2. Bearbeiten Sie die E-Mail-Adresse, an die Remote-Befehle zu senden sind.

HINWEIS

Die E-Mail-Adresse sollte **KEINE** lokale Domäne sein. Die Standardadresse lautet **rcommands@mailessentials.com**. Für die konfigurierte Adresse muss kein Postfach existieren. Der Domänenteil der Adresse muss jedoch eine vorhandene E-Mail-Adressdomäne angeben, für die beim DNS-Lookup des MX-Eintrags keine Fehlermeldung ausgegeben wird. Die kann auch ein öffentliches E-Mail-Konto sein, das Sie verwalten (z. B. Gmail oder Yahoo-Mail).

3. Optional können Sie die Remote-Befehle auch mit einfachen Schutzmaßnahmen gegen Missbrauch sichern:

» Sie können ein Kennwort angeben, das in die E-Mail eingefügt wird. Weitere Informationen finden Sie unter „Verwenden von Remote-Befehlen“ (Seite 162).

» Sie können festlegen, welche Benutzer E-Mails mit Remote-Befehlen verschicken dürfen.

4. Klicken Sie auf **Übernehmen**.

Verwenden von Remote-Befehlen

Remote-Befehle können von einem E-Mail-Client innerhalb der Domäne per E-Mail an GFI MailEssentials gesendet werden. Bedingungen zum Senden von Remote-Befehlen:

» Die E-Mail muss im Nur-Text-Format sein.

» Der Betreff der E-Mail ist leer.

» Die folgende Syntax muss für alle Befehle verwendet werden:

```
<Befehlsname>: <Parameter1>, <Parameter2>, <Parameter3>, … ;
```

Beispiel:`ADDBLIST: spammer@spam.com;`

» Im Textkörper einer E-Mail kann mehr als ein Befehl verwendet werden. Alle Befehle müssen durch ein Semikolon (;) voneinander getrennt sein.

» Falls für Remote-Befehle ein Kennwort festgelegt wird, geben Sie das Kennwort in die erste Zeile gemäß der folgenden Syntax ein:

```
PASSWORD: <gemeinsames>;
```

» Bei Befehlsnamen muss die Groß-/Kleinschreibung beachtet werden. Es wird empfohlen, nur GROSSSCHREIBUNG zu verwenden.

» Bedingungen wie `IF, AND, OR` werden nicht unterstützt.

» Remote-Befehle können nur verwendet werden, um Einträge hinzuzufügen. Sie dienen nicht zum Löschen oder Ändern vorhandener Einträge.

Stichwortbefehle

Verwenden Sie Stichwortbefehle, um Stichwörter oder Stichwortkombinationen in die Textkörper- oder Betrefflisten des Filters zur Stichwortprüfung einzufügen.

Verfügbare Befehle:

» ADDSUBJECT – Mit diesem Befehl werden der Datenbank für die Stichwortprüfung von Betreffzeilen neue Stichwörter hinzugefügt.

- Beispiel: ADDSUBJECT: Sex, Porno, Spam;

» ADDBODY – Mit diesem Befehl werden der Datenbank für die Stichwortprüfung des Textkörpers neue Stichwörter hinzugefügt.

- Beispiel: ADDBODY: kostenlos, „100 % umsonst“, „absolut umsonst“;

> **HINWEIS**
>
> Wenn Sie Ausdrücke eingeben, die aus mehr als einem Wort bestehen, setzen Sie sie in doppelte Anführungszeichen („ “).

Blocklist-Befehle

Mit Blocklist-Befehlen können Sie der E-Mail-Blocklist eine einzelne E-Mail-Adresse oder eine gesamte Domäne hinzufügen.

Verfügbare Befehle:

» `ADDBLIST: <E-Mail-Adresse>;`

- Beispiel: `ADDBLIST: user@somewhere.com;`

> **HINWEISE**
>
> 1. Um der Blocklist eine ganze Domäne hinzuzufügen, muss vor der Domäne ein Platzhalter gesetzt werden.
>
> **Beispiel:** `ADDBLIST: *@domain.com;`
>
> 2. Innerhalb des Domänennamens können keine Platzhalter verwendet werden.
>
> **Beispiel:**`ADDBLIST: *@*.domain.com;` ist ungültig und wird nicht akzeptiert.
>
> 3. Aus Sicherheitsgründen lässt sich in einer E-Mail nur ein `ADDBLIST`-Befehl verwenden, und nur eine Adresse kann als Befehlsparameter angegeben werden. Der Parameter ist entweder eine E-Mail-Adresse oder eine Domäne:
>
> **Beispiel:**`ADDBLIST: spammer@spam.com;` oder `ADDBLIST:*@spammers.org;`

Befehle für den Bayes'schen Filter

Sie können der Datenbank des Bayes'schen Filters Spam oder Ham (gültige E-Mail-Adressen) hinzufügen. Verfügbare Befehle:

Befehl	Beschreibung
ADDASSPAM	Weist den Bayes'schen Filter an, die E-Mail-Adresse als Spam zu klassifizieren.
ADDASGOODMAIL	Weist den Bayes'schen Filter an, die E-Mail-Adresse als HAM zu klassifizieren.

> **HINWEIS**
>
> Diese Befehle besitzen keine gesonderten Parameter, da der übrige Inhalt der Nachricht bereits als Parameter gilt.

Protokollieren von Remote-Befehlen

Um Änderungen an der Konfigurationsdatenbank über Remote-Befehle nachverfolgen zu können, werden alle E-Mails mit solchen Befehlen (selbst, wenn die E-Mails ungültig waren) im folgenden Verzeichnis gespeichert:

<GFI MailEssentials Installationspfad>\GFI\MailEssentials\AntiSpam\ADBRProcessed\

Der Dateiname jeder E-Mail besitzt folgende Formatierung:

» `<E-Mail-Adresse_des_Absenders>_SUCCESS_<Zeitstempel>.eml` - bei erfolgreicher Verarbeitung.

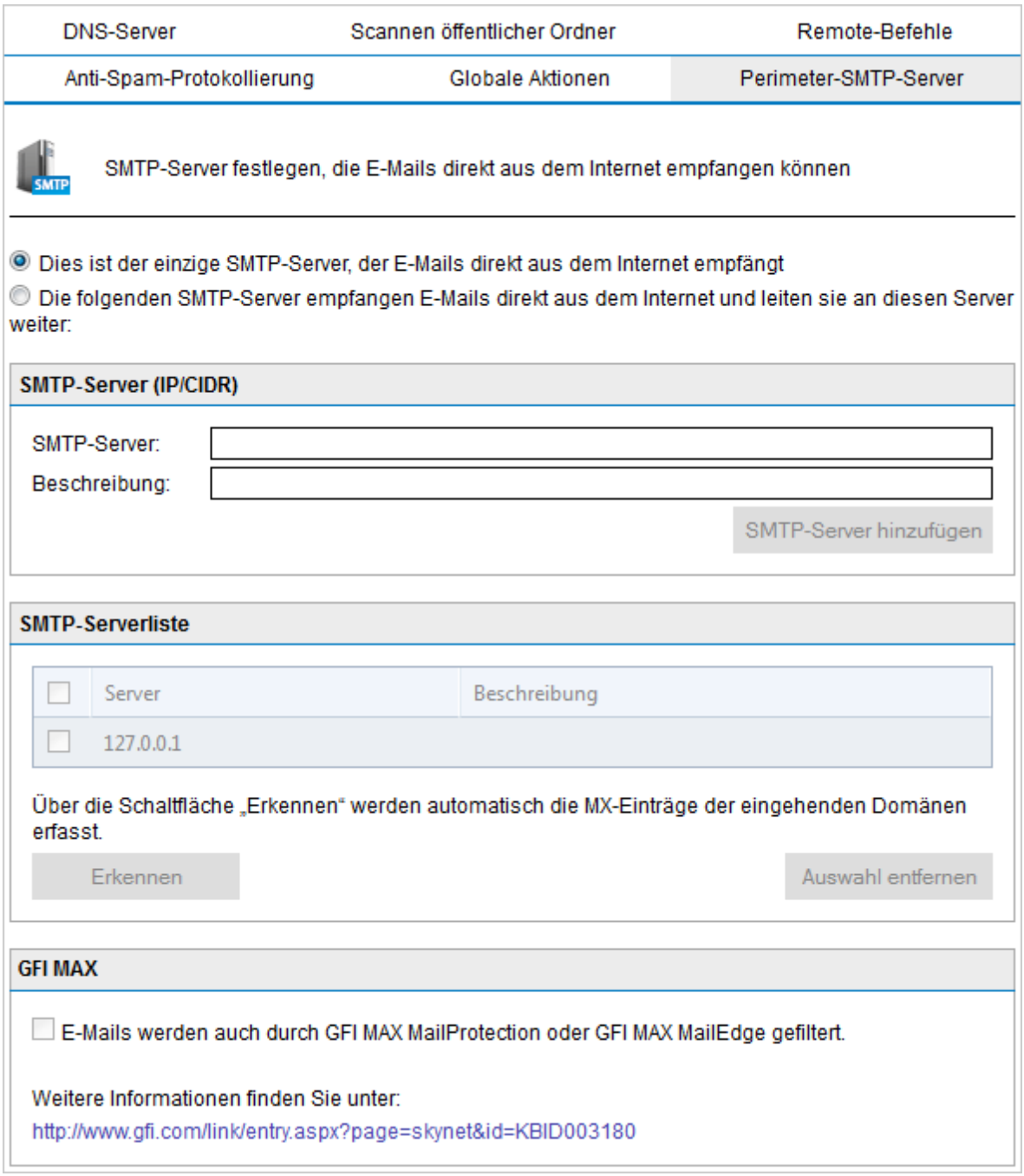
» `<E-Mail-Adresse_des_Absenders>_FAILED_<Zeitstempel>.eml` - bei fehlgeschlagener Verarbeitung.

> **HINWEIS**
>
> Der Zeitstempel hat das Format `jjjjmmtthhmmss`.

6.6.5 Perimeter-SMTP-Servereinstellungen

SMTP-Server, die E-Mails an den GFI MailEssentials-Server umleiten, müssen angegeben werden.

1. Wählen Sie in GFI MailEssentials Configuration die Optionen **Anti-Spam > Anti-Spam-Einstellungen** aus.



Screenshot 91: Perimeter-SMTP-Servereinstellungen

2. Konfigurieren Sie auf der Registerkarte **Perimeter-SMTP-Server** folgende Optionen:

Option	Beschreibung
Dies ist der einzige SMTP-Server, der E-Mails direkt aus dem Internet empfängt	Wählen Sie diese Option aus, wenn GFI MailEssentials auf dem einzigen SMTP-Server installiert ist, der externe E-Mails direkt aus dem Internet empfängt.

Option	Beschreibung
Die folgenden SMTP-Server empfangen E-Mails direkt aus dem Internet und leiten sie an diesen Server weiter	E-Mails werden von anderen SMTP-Servern an den GFI MailEssentials-Server weitergeleitet. Klicken Sie auf **Erkennen**, damit GFI MailEssentials automatisch SMTP-Server erkennt, indem die MX-Einträge der eingehenden Domänen abgefragt werden. Klicken Sie auf **SMTP-Server hinzufügen**, um die IP-Adressen aller anderen SMTP-Server, die E-Mails an den GFI MailEssentials-Server weiterleiten, manuell hinzuzufügen. **HINWEIS** Beim manuellen Hinzufügen von IP-Adressen von Perimeter-SMTP-Servern können Sie auch einen IP-Adressbereich in CIDR-Notation hinzufügen.
E-Mails werden auch durch GFI MAX MailProtection oder GFI MAX MailEdge gefiltert	Wählen Sie dies aus, wenn Sie die gehosteten E-Mail-Sicherheitsprodukte GFI MAX MailProtection oder GFI MAX MailEdge verwenden. Weitere Informationen finden Sie unter: http://go.gfi.com/?pageid=ME_MAXMPME

3. Klicken Sie auf **Übernehmen**.

6.7 SpamTag für Microsoft Outlook

Das Plug-In des GFI MailEssentials-SpamTag ist ein Add-On für Microsoft Outlook, das eine Symbolleiste auf den Computern der Endbenutzer installiert und so den Benutzern eine gewisse Kontrolle über die Verwaltung von Spam-E-Mails bietet. Das Plug-In synchronisiert auch die Microsoft Outlook Junk-Einstellungen mit GFI MailEssentials.

Dahingehend ermöglicht Microsoft Outlook Junk-Funktionen den Benutzern, Spam-E-Mails auf Client-Basis zu verwalten. Mit dem SpamTag-Plug-In können Benutzer ihre Spam-E-Mails auf Serverebene verwalten.

Der GFI MailEssentials-Administrator kann auswählen, welche der folgenden Funktionen aktiviert werden:

» Den Bayes'schen Analysefilter trainieren

» Absender und/oder Domänen zur persönlichen Blockliste oder Whitelist hinzufügen

» Synchronisieren Sie automatisch zulässige und blockierte Absender in Microsoft Outlook mit der persönlichen Whitelist bzw. Blocklist von GFI MailEssentials.

» Fügen Sie automatisch die Kontakte des Benutzers der persönlichen Whitelist hinzu.

HINWEIS

Benutzer, die Vollzugriff auf GFI MailEssentials haben, können ebenfalls Absender/Domänen zur globalen E-Mail-Blocklist und -Whitelist von GFI MailEssentials hinzufügen.

HINWEIS

Installieren Sie bei der Verwendung von SpamTag die WCF-HTTP-Aktivierung auf dem GFI MailEssentials-Server. Öffnen Sie dazu **Server Manager > Funktionen > Funktion hinzufügen > .NET Framework > WCF-Aktivierung > HTTP-Aktivierung**.

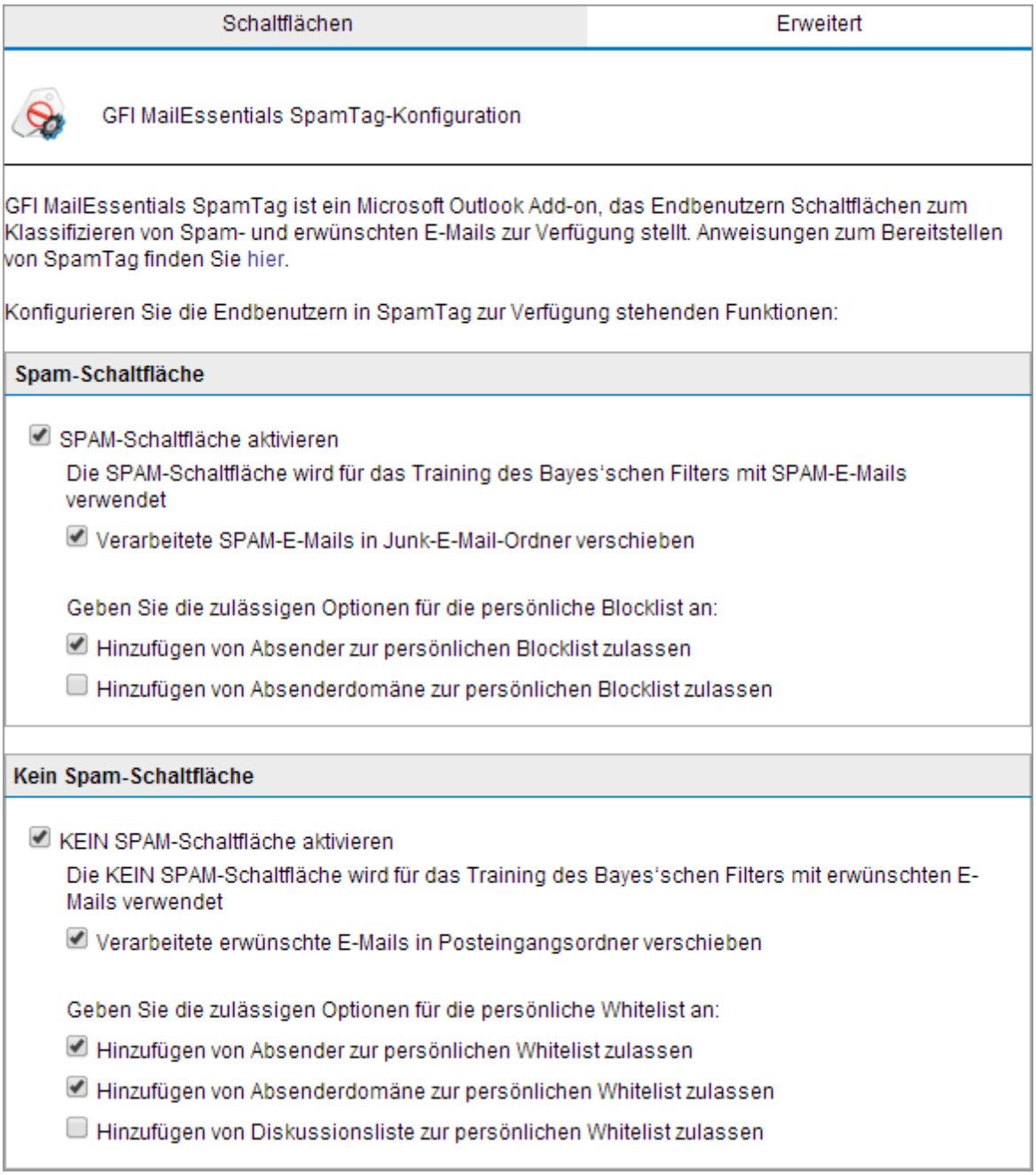
6.7.1 Auswählen von SpamTag-Funktionen

Der GFI MailEssentials-Administrator kann konfigurieren, welche Funktionen SpamTag-Benutzer verwenden können. Beispielsweise kann der Administrator Benutzer bevollmächtigen, Absender zur persönlichen Whitelist hinzuzufügen, ihnen aber untersagen, Domänen zur persönlichen Whitelist

hinzuzufügen. SpamTag kann auch konfiguriert werden, um die Microsoft Outlook Junk-Funktion zu überschreiben.

So konfigurieren Sie SpamTag-Funktionen:

1. Wählen Sie **Anti-Spam > SpamTag** aus.


Schaltflächen
Erweitert
GFI MailEssentials SpamTag-Konfiguration
GFI MailEssentials SpamTag ist ein Microsoft Outlook Add-on, das Endbenutzern Schaltflächen zum Klassifizieren von Spam- und erwünschten E-Mails zur Verfügung stellt. Anweisungen zum Bereitstellen von SpamTag finden Sie hier.
Konfigurieren Sie die Endbenutzern in SpamTag zur Verfügung stehenden Funktionen:
Spam-Schaltfläche
SPAM-Schaltfläche aktivieren
Die SPAM-Schaltfläche wird für das Training des Bayes'schen Filters mit SPAM-E-Mails verwendet
Verarbeitete SPAM-E-Mails in Junk-E-Mail-Ordner verschieben
Geben Sie die zulässigen Optionen für die persönliche Blocklist an:
Hinzufügen von Absender zur persönlichen Blocklist zulassen
Hinzufügen von Absenderdomäne zur persönlichen Blocklist zulassen
Kein Spam-Schaltfläche
KEIN SPAM-Schaltfläche aktivieren
Die KEIN SPAM-Schaltfläche wird für das Training des Bayes'schen Filters mit erwünschten E-Mails verwendet
Verarbeitete erwünschte E-Mails in Posteingangsordner verschieben
Geben Sie die zulässigen Optionen für die persönliche Whitelist an:
Hinzufügen von Absender zur persönlichen Whitelist zulassen
Hinzufügen von Absenderdomäne zur persönlichen Whitelist zulassen
Hinzufügen von Diskussionsliste zur persönlichen Whitelist zulassen

2. Konfigurieren Sie im Bereich **Spam-Schaltfläche** die Funktionen für falsch-positive Ergebnisse, d. h. wenn Spam-E-Mails nicht als solche erkannt werden:

Option	Beschreibung
SPAM-Schaltfläche aktivieren	Die Schaltfläche **Spam** wird in SpamTag angezeigt. Wenn Sie darauf klicken, trainiert die ausgewählte E-Mail den Filter der Bayes'schen Analyse.
Verarbeitete SPAM-E-Mails in Junk-E-Mail-Ordner verschieben	Beim Klicken auf **Spam** wird die ausgewählte E-Mail automatisch in den Junk-E-Mail-Ordner von Microsoft Outlook verschoben.

Option	Beschreibung
Hinzufügen von Absender zur persönlichen Blocklist zulassen	Unter der Schaltfläche **Spam** wird eine Unteroption angezeigt, mit der Benutzer die E-Mail-Adresse des Absenders ihrer persönlichen Blocklist hinzufügen können. Damit Sie diese Option verwenden können, muss die persönliche Blocklist aktiviert sein.
Hinzufügen von Absenderdomäne zur persönlichen Blocklist zulassen	Unter der Schaltfläche **Spam** wird eine Unteroption angezeigt, mit der Benutzer die Domäne des Absenders ihrer persönlichen Blocklist hinzufügen können. Damit Sie diese Option verwenden können, muss die persönliche Blocklist aktiviert sein.

3. Konfigurieren Sie im Bereich **Schaltfläche „Kein Spam“** die Funktionen für falsch-positive Ergebnisse, d. h. wenn erwünschte E-Mails fälschlicherweise als Spam erkannt werden:

Option	Beschreibung
KEIN SPAM-Schaltfläche aktivieren	Die Schaltfläche **Kein Spam** wird in SpamTag angezeigt. Wenn Sie darauf klicken, trainiert die ausgewählte E-Mail den Filter der Bayes‘schen Analyse.
Verarbeitete erwünschte E-Mails in Posteingangsordner verschieben	Beim Klicken auf **Kein Spam** wird die ausgewählte E-Mail automatisch in den Posteingang von Microsoft Outlook verschoben.
Hinzufügen von Absender zur persönlichen Whitelist zulassen	Unter der Schaltfläche **Kein Spam** wird eine Unteroption angezeigt, mit der Benutzer die E-Mail-Adresse des Absenders ihrer persönlichen Whitelist hinzufügen können. Damit Sie diese Option verwenden können, muss die persönliche Whitelist aktiviert sein.
Hinzufügen von Absenderdomäne zur persönlichen Whitelist zulassen	Unter der Schaltfläche **Kein Spam** wird eine Unteroption angezeigt, mit der Benutzer die Domäne des Absenders ihrer persönlichen Whitelist hinzufügen können. Damit Sie diese Option verwenden können, muss die persönliche Whitelist aktiviert sein.
Hinzufügen von Diskussionsliste zur persönlichen Whitelist zulassen	Unter der Schaltfläche **Kein Spam** wird eine Unteroption angezeigt, mit der Benutzer Newsletter/Diskussionslisten der Whitelist hinzufügen können. Damit Sie diese Option verwenden können, muss die persönliche Whitelist aktiviert sein.

4. Konfigurieren Sie auf der Registerkarte **Erweitert** die folgenden erweiterten Optionen.

Option	Beschreibung
Die Junk-Mail-Einstellungen von Outlook in die persönliche Blocklist bzw. Whitelist importieren	Importiert die Adressen der Microsoft Outlook-Listen „Sichere Absender“ und „Blockierte Absender“ in die persönliche Whitelist und Blocklist von GFI MailEssentials. Die Listen „Sichere Absender“ und „Blockierte Absender“ in Microsoft Outlook finden Sie unter **Junk > Junk-E-Mail-Optionen**. **HINWEIS:** Importe werden automatisch von SpamTag alle 2 Stunden im Hintergrund ausgeführt, d. h. der Benutzer muss keine Optionen konfigurieren und es wird nichts auf dem Bildschirm angezeigt. **HINWEIS:** Wenn der Benutzer Microsoft Outlook verwendet, das auf einem batteriebetriebenen Gerät wie einem Laptop oder einem Tablet installiert ist, wird die automatische Synchronisierung nicht ausgeführt, um Batterie zu sparen.
Kontakte von Outlook in die persönliche Whitelist importieren	Importiert die Liste der Microsoft Outlook-Kontakte in die persönliche Whitelist. **HINWEIS:** Importe werden automatisch von SpamTag alle 2 Stunden im Hintergrund ausgeführt, d. h. der Benutzer muss keine Optionen konfigurieren und es wird nichts auf dem Bildschirm angezeigt. **HINWEIS:** Wenn der Benutzer Microsoft Outlook verwendet, das auf einem batteriebetriebenen Gerät wie einem Laptop oder einem Tablet installiert ist, wird die automatische Synchronisierung nicht ausgeführt, um Batterie zu sparen.

Option	Beschreibung
Microsoft Outlook Junk-Einstellungen überschreiben	Bei Auswahl dieser Option überschreiben die in SpamTag aktivierten Optionen die entsprechenden Einstellungen in Microsoft Outlook Junk, um sicherzustellen, dass auf dem Client nur ein Anti-Spam-Verwaltungssystem verwendet wird. Wenn Benutzer eine Microsoft Outlook Junk-Option verwenden, wird stattdessen die entsprechende SpamTag-Funktion ausgeführt. Wenn Benutzer in Outlook Junk beispielsweise auf **Absender niemals blockieren** klicken, wird stattdessen die SpamTag-Funktion **Kein Spam** ausgeführt. **HINWEIS:** Wenn eine bestimmte Option nicht in SpamTag aktiviert ist und der Benutzer die entsprechende Funktion in Outlook Junk verwendet, findet keine Aktion statt. Wenn beispielsweise in SpamTag die Schaltfläche „Kein Spam“ nicht aktiviert ist, passiert nichts, wenn der Benutzer in Outlook Junk auf **Absender niemals blockieren** klickt.
Konsolenschaltfläche ausblenden	Blendet die Konsolenschaltfläche in der SpamTag-Symbolleiste aus. Es ist kein direkter Zugriff auf die GFI MailEssentials-Konsole möglich, aber Benutzer können sich dennoch durch manuelle Eingabe der URL in den Browser anmelden. Die dem Benutzer zur Verfügung stehenden Einstellungen in der GFI MailEssentials-Konsole hängen von den Active Directory-Berechtigungen oder andere benutzerdefinierten Zugriffssteuerungseinstellungen ab. Weitere Informationen finden Sie unter „Zugriffssteuerung“ (Seite 251).

5. Klicken Sie auf **Übernehmen**.

> **WICHTIG**
>
> SpamTag prüft, welche Funktionen in GFI MailEssentials aktiviert bzw. deaktiviert, wenn Microsoft Outlook gestartet wird. Nach der Änderung der obigen Einstellungen muss Microsoft Outlook neu gestartet werden, um die Änderungen zu übernehmen.

6.7.2 SpamTag-Anforderungen

Die Computer, auf denen SpamTag installiert wird, müssen mindestens den folgenden Spezifikationen entsprechen:

Hardware	» Prozessor – 1 GHz oder mehr » Arbeitsspeicher – Min. 512 MB (2 GB empfohlen) » Physischer Speicher – 50 MB physischer Speicher dediziert für SpamTag
Unterstützte Betriebssysteme	» Windows® 8 und 8.1 » Windows® 7 » Windows® Vista » Windows® XP » Windows® Server 2012 » Windows® Server 2008 » Windows® Server 2003
Unterstützte Versionen von Microsoft Outlook®	» Microsoft Outlook® 2013 (x86- und x64-Versionen) » Microsoft Outlook® 2010 (x86- und x64-Versionen, Service Packs 1 und 2) » Microsoft Outlook® 2007 (Service Packs 1 und 2) » Microsoft Outlook® 2003 (Service Packs 1, 2, 3 und 4)
Verbindung mit GFI MailEssentials	SpamTag verbindet sich auf Port 80 über HTTP mit GFI MailEssentials. Um die Verbindung vom Client-Browser aus zu bestätigen, stellen Sie sicher, dass Sie die GFI MailEssentials-URL öffnen können.
Weitere Software	Microsoft .Net Framework 4 – Dies wird automatisch heruntergeladen und installiert, wenn es noch nicht installiert ist.

6.7.3 Manuelles Installieren von SpamTag

Führen Sie das SpamTag-Installationsprogramm auf dem Client-Computer aus, um SpamTag manuell zu installieren.

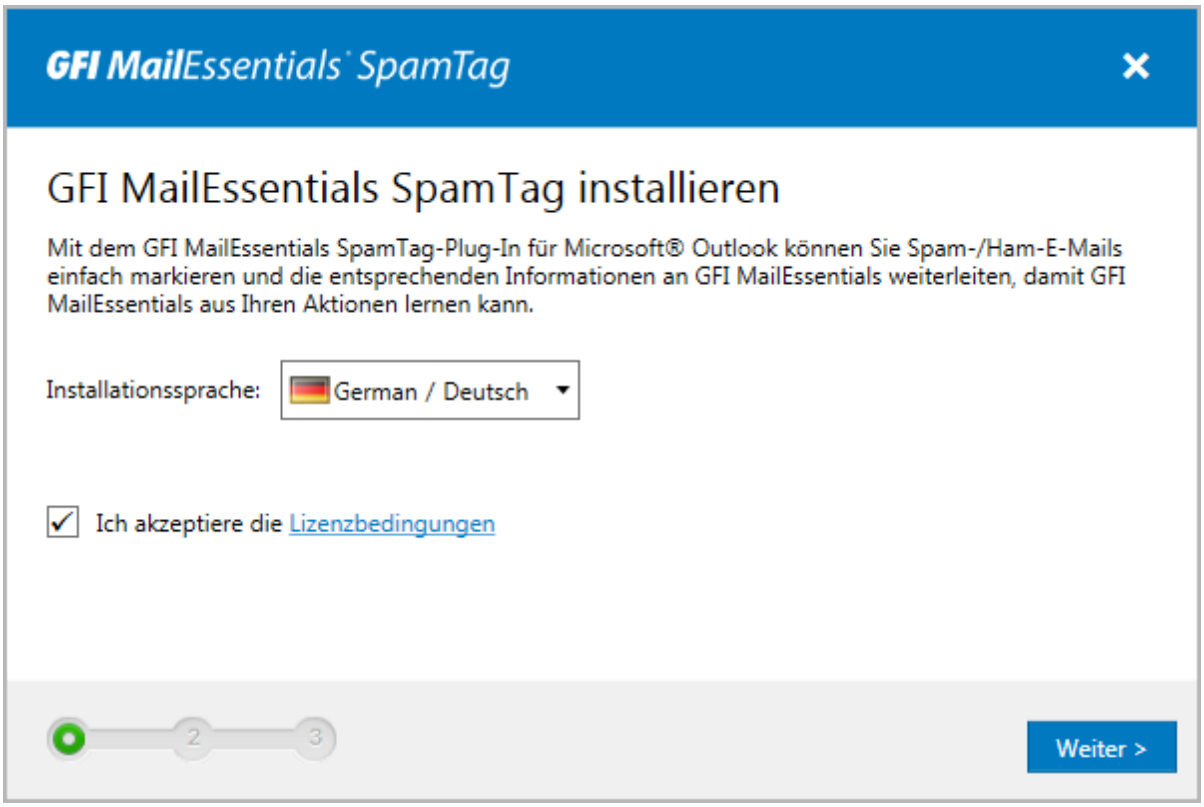
1. Das Installationsprogramm finden Sie unter **<GFI MailEssentials-Installationsordner>/Outlook**.

2. Kopieren Sie die Datei **GFIMailEssentialsSpamTag.exe** auf den Computer, auf dem SpamTag installiert werden soll.

3. Microsoft Outlook schließen

4. Klicken Sie mit der rechten Maustaste auf das Installationsprogramm, und wählen Sie **Als Administrator ausführen**.

5. Wählen Sie auf dem ersten Bildschirm die Sprache für die Installation aus.


GFI MailEssentials SpamTag
GFI MailEssentials SpamTag installieren
Mit dem GFI MailEssentials SpamTag-Plug-In für Microsoft® Outlook können Sie Spam-/Ham-E-Mails einfach markieren und die entsprechenden Informationen an GFI MailEssentials weiterleiten, damit GFI MailEssentials aus Ihren Aktionen lernen kann.
Installationssprache:
German / Deutsch
Ich akzeptiere die Lizenzbedingungen
2
3
Weiter >

Screenshot 92: SpamTag-Installationssprache und -Lizenzbedingungen

6. Lesen Sie die **Lizenzbedingungen**, und wenn Sie zustimmen, wählen Sie **Ich bestätige, dass ich die Allgemeinen Nutzungsbedingungen gelesen habe und stimmen ihnen zu**. Klicken Sie auf **Weiter**.

7. Geben Sie die URL ein, die zur Verbindung mitGFI MailEssentials verwendet wird. Beispiel: `http://192.168.1.2/MailEssentials` oder `http://mygfiserver.mydomin.com/MailEssentials`. Warten Sie darauf, dass das Installationsprogramm die Verbindung mit GFI MailEssentials über die angegebene URL herstellt, und klicken Sie auf **Weiter**.

8. Geben Sie den Speicherort an, an dem SpamTag installiert werden soll, und klicken Sie auf **Installieren**.

9. Klicken Sie nach Abschluss auf **Fertig stellen**.

10. Starten Sie Microsoft Outlook, und geben Sie die Anmeldeinformationen des Benutzers ein.

SpamTag ist nun im Menüband der Microsoft Outlook-Startseite (ab Version 2007) oder in der Symbolleiste (Version 2003) verfügbar.

Klicken Sie für weitere Informationen zu SpamTag auf **Hilfe**.

6.7.4 Installieren von SpamTag über GPO

Dieser Abschnitt hilft Ihnen bei der automatischen Installation von GFI MailEssentials-SpamTag auf mehreren Computern über GPO. Wählen Sie Ihre Domänencontroller-Umgebung:

» Windows Server 2008 und 2012

» Windows Server 2003

Installieren von SpamTag über GPO unter Windows Server 2008 und 2012

Schritt 1: MSI- und ADM-Dateien vorbereiten

1. Öffnen Sie auf dem GFI MailEssentials-Server den GFI MailEssentials-Installationsordner und anschließend den **Outlook**-Unterordner.

2. Kopieren Sie die MSI- und ADM-Dateien in einen freigegebenen Ordner, auf den alle Benutzer zugreifen können, bei denen SpamTag installiert sein wird. Stellen Sie sicher, dass Benutzer zumindest Leserechte für diesen Ordner haben.

Schritt 2: SpamTag bereitstellen

1. Öffnen Sie auf dem Domänencontroller den **Server Manager**.

2. Erweitern Sie **Server Manager > Funktionen > Gruppenrichtlinienverwaltung > Gesamtstruktur > Domänen > *Domänenname***. Klicken Sie mit der rechten Maustaste auf den Domänennamen oder eine Organisationseinheit, und wählen Sie die Option **Ein GPO in dieser Domäne erstellen und hiermit verknüpfen...** aus.

3. Geben Sie einen Namen für das neue Gruppenrichtlinienobjekt (Group Policy Object, GPO) ein. Beispiel: `SpamTag von GFI MailEssentials`. Klicken Sie auf **OK**.

4. Klicken Sie mit der rechten Maustaste auf das neu erstellte GPO, und wählen Sie **Bearbeiten**.

5. Erweitern Sie im Fenster **Gruppenrichtlinienmanagement-Editor** die Option **Computerkonfiguration > Richtlinien > Softwareeinstellungen > Softwareinstallation**. Klicken Sie mit der rechten Maustaste auf **Softwareinstallation > Neu > Paket**, um das GPO so zu konfigurieren, dass es bei der Anmeldung installiert wird.

6. Geben Sie den Netzwerkpfad des freigegebenen Ordners ein, der das SpamTag-MSI-Paket enthält. Klicken Sie auf **OK**.

> **HINWEIS**
>
> Die Auswahl des Speicherorts der MSI-Datei muss über „Netzwerkstandorte“ erfolgen, damit der Freigabename des gemeinsamen Verzeichnisses in GFI MailEssentials nicht den lokalen, sondern den vollständigen Netzwerkpfad enthält.

7. Wählen Sie im Popup-Fenster **Software bereitstellen** die Option **Zugewiesen**, und klicken Sie auf **OK**.

8. Das neue Paket wird dann unter **Softwareinstallation** hinzugefügt.

9. Klicken Sie mit der rechten Maustaste auf **Computerkonfiguration > Richtlinien > Administrative Vorlagen**, und wählen Sie **Alle Aufgaben > Vorlage hinzufügen/entfernen**.

10. Klicken Sie auf **Hinzufügen**, und öffnen Sie den freigegebenen Ordner, der **spamtag.adm** enthält.

11. Klicken Sie auf **Schließen**.

12. Erweitern Sie **Computerkonfiguration > Richtlinien > Administrative Vorlagen > Klassische administrative Vorlage (ADM) > SpamTag von GFI MailEssentials**.

13. Doppelklicken Sie im rechten Bereich auf die Richtlinie **DefaultWebServiceUrl**, und wählen Sie **Aktiviert** aus. Geben Sie unter **GFI MailEssentials-Portal-Website-Adresse** die öffentliche URL von GFI MailEssentials ein. Computer, auf denen SpamTag bereitgestellt werden soll, müssen sich mit dieser URL über ihren Webbrowser verbinden können. Anderenfalls kann sich SpamTag nicht mit GFI MailEssentials verbinden.

14. Klicken Sie optional auf **Vorherige Einstellungen**, um die Standardsprache von SpamTag geändert. Klicken Sie auf **Aktiviert**, und ändern Sie den Wert **Standardsprache**.

15. Klicken Sie auf **OK**.

Schritt 3: Installation überprüfen

Die Einrichtung sollte damit abgeschlossen sein. SpamTag wird nach dem nächsten Neustart eines Clientcomputers installiert.

Prüfen Sie nach der Installation, ob die SpamTag-Symbolleiste in Microsoft Outlook® angezeigt wird und sie sich erfolgreich mit GFI MailEssentials verbindet.

Installieren von SpamTag über GPO unter Windows Server 2003

Schritt 1: MSI- und ADM-Dateien vorbereiten

1. Öffnen Sie auf dem GFI MailEssentials-Server den GFI MailEssentials-Installationsordner und anschließend den **Outlook**-Unterordner.

2. Kopieren Sie die MSI- und ADM-Dateien in einen freigegebenen Ordner, auf den alle Benutzer zugreifen können, bei denen SpamTag installiert sein wird. Stellen Sie sicher, dass Benutzer zumindest Leserechte für diesen Ordner haben.

Schritt 2: SpamTag bereitstellen

1. Geben Sie in der Befehlszeile `mmc.exe` ein, um die Microsoft Management Console zu starten.

2. Wählen Sie **Datei > Snap-In hinzufügen/entfernen…** aus, und klicken Sie auf **Hinzufügen...**.

3. Wählen Sie das Snap-In **Gruppenrichtlinienobjekt-Editor** aus, und klicken Sie auf **Hinzufügen**.

4. Klicken Sie auf **Durchsuchen...**, und wählen Sie die zu bearbeitende Domänenrichtlinie aus.

5. Wählen Sie die Domänenrichtlinie aus, und klicken Sie auf **OK**.

6. Klicken Sie auf **Fertig stellen**, um das Dialogfeld „Gruppenrichtlinienobjekt auswählen“ zu schließen. Klicken Sie auf **Schließen**, um das Dialogfeld „Eigenständiges Snap-In hinzufügen“ zu schließen. Klicken Sie anschließend auf **OK**, um das Dialogfeld „Snap-In hinzufügen/entfernen“ zu schließen und zur Microsoft Management Console zurückzukehren.

7. Wählen Sie **Konsolenstamm > <Domänenrichtlinie> > Benutzerkonfiguration**, klicken Sie mit der rechten Maustaste auf **Administrative Vorlagen**, und wählen Sie **Vorlagen hinzufügen/entfernen...** aus.

8. Klicken Sie auf **Hinzufügen...**, und suchen Sie die ADM-Datei im Ordner, der in Schritt 1 freigegeben wurde. Klicken Sie auf **Öffnen**.

9. Klicken Sie auf **Schließen**, um zur Microsoft Management Console zurückzukehren.

10. Erweitern Sie **Konsolenstamm > <Domänenrichtlinie> > Benutzerkonfiguration > Administrative Vorlagen > GFI-Anwendungen**.

11. Doppelklicken Sie im rechten Bereich auf die Richtlinie **DefaultWebServiceUrl**, und wählen Sie **Aktiviert** aus. Geben Sie die öffentliche URL von GFI MailEssentials ein. Computer, auf denen SpamTag bereitgestellt werden soll, müssen sich mit dieser URL über ihren Webbrowser verbinden können. Anderenfalls kann sich SpamTag nicht mit GFI MailEssentials verbinden.

12. Klicken Sie optional auf **Vorherige Einstellungen**, um die Standardsprache von SpamTag geändert. Klicken Sie auf **Aktiviert**, und ändern Sie den Wert **Standardsprache**.

13. Klicken Sie auf **OK**.

14. Wählen Sie **Konsolenstamm > <*Domänenrichtlinie*> > Benutzerkonfiguration > Softwareeinstellungen**.

15. Klicken Sie mit der rechten Maustaste auf **Softwareinstallation**, und wählen Sie **Neu > Paket…** aus.

16. Suchen Sie im Dialogfeld **Öffnen** nach der Freigabe, in der die MSI-Datei in Schritt 1 gespeichert ist.

> **HINWEIS**
>
> Die Auswahl des Speicherorts der MSI-Datei muss über „Netzwerkstandorte“ erfolgen, damit der Freigabename des gemeinsamen Verzeichnisses in GFI MailEssentials nicht den lokalen, sondern den vollständigen Netzwerkpfad enthält.

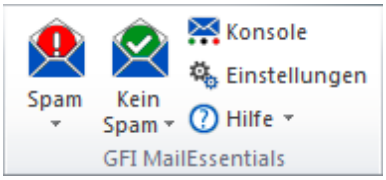
17. Wählen Sie die Bereitstellungsoption **Zugewiesen**, und klicken Sie auf **OK**.

Schritt 3: Installation überprüfen

Die Einrichtung sollte damit abgeschlossen sein. SpamTag wird nach dem nächsten Neustart eines Clientcomputers installiert.

Prüfen Sie nach der Installation, ob die SpamTag-Symbolleiste in Microsoft Outlook® angezeigt wird und sie sich erfolgreich mit GFI MailEssentials verbindet.

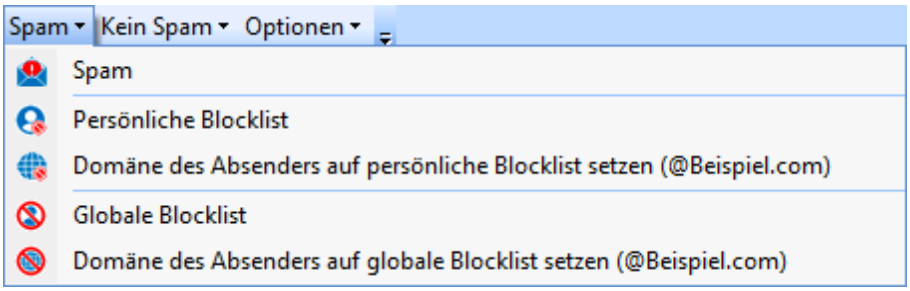
6.7.5 Verwenden von SpamTag



Screenshot 93: SpamTag in Microsoft Outlook 2010

Informationen zur Verwendung von SpamTag finden Sie in der integrierten Hilfe, indem Sie in SpamTag auf **Hilfe** klicken.

Die Hilfe zeigt automatisch Informationen zu den Funktionen an, die vom Administrator auf der SpamTag-Einstellungsseite aktiviert wurden.



Screenshot 94: SpamTag in Microsoft Outlook 2003

6.8 Scannen öffentlicher Ordner

Spam-Techniken entwickeln sich kontinuierlich weiter, daher kann es vorkommen, dass einzelne Spam-Nachrichten trotz aller Anti-Spam-Filter in den Posteingang des Empfängers gelangen. Durch das Scannen öffentlicher Ordner können Benutzer E-Mails manuell als Spam klassifizieren und GFI MailEssentials mit Spam-Mustern 'trainieren', damit ähnliche E-Mails als Spam erkannt werden. Es ist aber auch möglich, E-Mails zur Whitelist hinzuzufügen.

WICHTIG

Es wird dringend empfohlen, SpamTag von GFI MailEssentials anstelle des Scannens öffentlicher Ordner zu verwenden, wenn Netzwerk-Clients Microsoft Outlook als E-Mail-Client verwenden. Weitere Informationen finden Sie unter „SpamTag für Microsoft Outlook“ (Seite 166).

Funktionsweise:

1. Wird eine falsch klassifizierte E-Mail (falsch-positiv oder falsch-negativ) identifiziert, kann der Benutzer diese in den entsprechenden öffentlichen Ordner von GFI AntiSpam verschieben. Weitere Informationen finden Sie unter „Scannen öffentlicher Ordner verwenden“ (Seite 178).

2. Durch das Scannen öffentlicher Ordner werden E-Mails aus den öffentlichen Ordnern von GFI AntiSpam abgerufen und zur Whitelist/Blocklist bzw. den HAM-/SPAM-Datenbanken hinzugefügt.

Die öffentlichen Ordner von GFI AntiSpam müssen auf dem Mailserver erstellt und konfiguriert werden. Weitere Informationen finden Sie unter „Scannen öffentlicher Ordner aktivieren“ (Seite 174).

6.8.1 Scannen öffentlicher Ordner aktivieren

Folgen Sie den Anweisungen in den folgenden Abschnitten, um das Scannen öffentlicher Ordner zu aktivieren:

- Scannen öffentlicher Ordner für Microsoft® Exchange-Server einrichten
- Ein dediziertes Benutzerkonto für Microsoft® Exchange Server 2003 konfigurieren
- Ein dediziertes Benutzerkonto für Microsoft® Exchange Server 2007/2010 konfigurieren
- Benutzerbeiträge in GFI AntiSpam-Ordnern ausblenden

HINWEIS

Sie können GFI MailEssentials auch zusammen mit Lotus Domino verwenden. Weitere Informationen finden Sie unter „Lotus Domino“ (Seite 31).

Scannen öffentlicher Ordner für Microsoft® Exchange-Server einrichten

1. Wählen Sie in der Konfigurationskonsole von GFI MailEssentials die Optionen **Anti-Spam > Anti-Spam-Einstellungen** aus. Wählen Sie die Registerkarte **Scannen öffentlicher Ordner** aus.

2. Wählen Sie **Scannen öffentlicher Ordner aktivieren** aus, und aktivieren Sie in der Liste **Öffentliche Ordner abrufen über** die entsprechende Option:

- **Exchange Server 2003** – Wählen Sie MAPI, IMAP oder WebDAV aus.
- **Exchange Server 2007** – Wählen Sie WebDAV oder Web Services aus.
- **Exchange Server 2010** – Wählen Sie Web Services aus.

Die Optionen werden in der unten angeführten Tabelle beschrieben.

Option	Beschreibung
MAPI	MAPI kann nur verwendet werden, wenn GFI MailEssentials auf demselben Computer wie Microsoft® Exchange Server installiert ist. Es sind keine weiteren Einstellungen erforderlich.
IMAP	Erfordert den Microsoft® Exchange IMAP-Dienst. IMAP ermöglicht Remote-Scans für öffentliche Ordner und funktioniert gut in Umgebungen mit Firewalls. Zudem ist eine Verwendung mit anderen Mailservern möglich, die IMAP unterstützen. Erforderliche Parameter: » Mailservername » Portnummer (Standard-IMAP-Port ist 143) » Benutzername/Kennwort » Wählen Sie **SSL verwenden** aus, um eine sichere Verbindung zu verwenden.
WebDAV	Geben Sie Mailservername, Port (Standard-WebDAV-Port ist 80), Benutzername/Kennwort und Domäne an. Aktivieren Sie **SSL verwenden**, um eine sichere Verbindung zu verwenden. Öffentliche Ordner sind standardmäßig im virtuellen Verzeichnis 'public' verfügbar. Bearbeiten Sie den Text im Feld **URL**, wenn diese Einstellung geändert wurde, um den Namen des richtigen virtuellen Verzeichnisses für den Zugriff auf die öffentlichen Ordner anzugeben.
Web Services	Geben Sie folgende Informationen an: » **Server** – Name des Mailservers » **Domäne** – Lokale Domäne **HINWEIS** Wenn sowohl eine lokale als auch eine öffentliche Domäne vorhanden sind, verwenden Sie die lokale Domäne. » **Port** – Standardport für Web Services (80, bei SSL 443). » **Benutzername/Kennwort** – Verwenden Sie Anmeldeinformationen mit administrativen Berechtigungen, oder erstellen Sie ein dediziertes Benutzerkonto mit Microsoft® Exchange® Management Shell, indem Sie folgenden Befehl eingeben, um die erforderlichen Berechtigungen hinzuzufügen: `Add-ADPermission -identity "Postfachspeicher" -User NewUser -AccessRights GenericALL` Ersetzen Sie `Postfachspeicher` mit dem Namen des Postfachspeichers, der die Benutzerpostfächer enthält, und ersetzen Sie `NewUser` mit dem Benutzernamen des erstellten Benutzers. » **SSL verwenden** – Wählen Sie diese Option aus, wenn für Exchange Web Services eine sichere Verbindung erforderlich ist. Web Services erfordern standardmäßig SSL. » **URL** – Öffentliche Ordner sind standardmäßig im virtuellen Verzeichnis 'EWS/exchange.asmx' verfügbar. Bearbeiten Sie den Text im URL-Feld, wenn diese Einstellung geändert wurde, um den Namen des richtigen virtuellen Verzeichnisses für den Zugriff auf die öffentlichen Ordner anzugeben. **HINWEIS** Es wird empfohlen, die Einstellungen durch Eingeben der URL in einem Webbrowser manuell zu überprüfen. Bei diesem Vorgang sollte die XML-Datei **services.wsdl** geladen werden.

3. Klicken Sie auf **Jetzt scannen**, um die öffentlichen Ordner automatisch zu erstellen.

4. Klicken Sie auf **Testen**, wenn Sie IMAP, WebDAV oder Web Services einrichten. Eine Meldung zeigt, ob der Test erfolgreich war. Schlägt der Test fehl, kontrollieren/aktualisieren Sie die Zugangsdaten, und versuchen Sie es erneut.

5. Klicken Sie auf **Übernehmen**.

Ein dediziertes Benutzerkonto für Microsoft® Exchange Server 2003 konfigurieren

Ist GFI MailEssentials in einer DMZ installiert, sollte aus Sicherheitsgründen ein dediziertes Benutzerkonto erstellt werden, über das E-Mails aus den öffentlichen Ordnern abgerufen/gescannt werden.

1. Richten Sie einen neuen Active Directory-Benutzer ein.

2. Erweitern Sie im Microsoft® Exchange-System-Manager den Knoten **Ordner > Öffentliche Ordner**.

3. Klicken Sie mit der rechten Maustaste auf den öffentlichen Ordner **GFI AntiSpam-Ordner**, und wählen Sie **Eigenschaften** aus.

4. Klicken Sie auf die Registerkarte **Berechtigungen**, und wählen Sie **Client-Berechtigungen** aus.

5. Klicken Sie auf **Hinzufügen…**, wählen Sie die Option für neue Benutzer aus, und klicken Sie auf **OK**.

6. Wählen Sie den neuen Benutzer in der Liste der Client-Berechtigungen aus, und weisen Sie ihm aus der angezeigten Liste die Rolle **Besitzer** zu. Stellen Sie sicher, dass alle Kontrollkästchen aktiviert und die Optionsfelder auf **Alle** eingestellt sind.

7. Klicken Sie auf **OK**, um die Konfiguration abzuschließen.

8. Klicken Sie im Microsoft® Exchange-System-Manager mit der rechten Maustaste auf **GFI AntiSpam-Ordner**, und wählen Sie **Alle Aufgaben > Einstellungen weitergeben** aus.

> **HINWEIS**
>
> Bei Microsoft® Exchange Server 2003 SP2 klicken Sie mit der rechten Maustaste auf **GFI AntiSpam-Ordner**, und wählen Sie **Alle Aufgaben > Einstellungen verwalten** aus.

9. Wählen Sie **Ordnerrechte oder Clientberechtigungen ändern** aus und klicken Sie auf **OK** oder **Weiter**.

10. Geben Sie die Anmeldeinformationen des neuen Hauptbenutzerkontos an, das in Schritt 1 erstellt wurde, und testen Sie die Konfiguration, um sicherzustellen, dass die Berechtigungen korrekt sind.

Ein dediziertes Benutzerkonto für Microsoft® Exchange Server 2007/2010 konfigurieren

Wenn Sie ein dediziertes Benutzerkonto zum Abrufen der E-Mails aus den öffentlichen GFI AntiSpam-Ordnern konfigurieren, muss der Benutzer für diese Ordner das Zugriffsrecht ‘Besitzer’ haben.

1. Richten Sie einen neuen Active Directory-(Haupt-)Benutzer ein.

2. Melden Sie sich mit Administratorrechten bei Microsoft® Exchange Server an.

3. Öffnen Sie die **Microsoft® Exchange-Verwaltungsshell**, und geben Sie den folgenden Befehl ein:

```
Get-PublicFolder -Identity "\GFI AntiSpam-Ordner" -Recurse | ForEach-
Object {Add-PublicFolderClientPermission -Identity $_.Identity -User
"BENUTZERNAME" -AccessRights owner -Server "SERVERNAME"}
```

Geben Sie für `BENUTZERNAME` und `SERVERNAME` die entsprechenden Daten des betreffenden Active Directory-Benutzers ein.

Beispiel:

```
Get-PublicFolder -Identity "\GFI AntiSpam-Ordner" -Recurse | ForEach-
Object {Add-PublicFolderClientPermission -Identity $_.Identity -User
"mesuser" -AccessRights owner -Server "exch07"}
```

Benutzerbeiträge in GFI AntiSpam-Ordnern ausblenden

Aus Gründen des Datenschutzes und der Sicherheit wird dringend empfohlen, Benutzerbeiträge auszublenden, die in GFI AntiSpam-Ordnern erstellt wurden. Auf diese Weise können Benutzer in den Ordnern Beiträge erstellen, die vorhandenen Beiträge jedoch nicht anzeigen (auch nicht die selbst erstellten). So konfigurieren Sie Benutzerrechte und blenden Beiträge für nicht berechtigte Benutzer aus:

Microsoft® Exchange 2003

1. Erweitern Sie im Microsoft® Exchange-System-Manager den Knoten **Ordner > Öffentliche Ordner**.

2. Klicken Sie mit der rechten Maustaste auf den öffentlichen Ordner **GFI AntiSpam-Ordner**, und wählen Sie **Eigenschaften** aus.

3. Wählen Sie die Registerkarte **Berechtigungen** aus, und klicken Sie auf **Client-Berechtigungen**.

4. Klicken Sie auf **Hinzufügen...**, wählen Sie den Benutzer/die Gruppe aus, die Beiträge nicht einsehen dürfen, und klicken Sie auf **OK**.

5. Wählen Sie den Benutzer/die Gruppe aus, die Sie zuvor in Liste der Client-Berechtigungen konfiguriert haben, und legen Sie seine/ihre Rolle als **Teilnehmer** fest.

6. Nur das Kontrollkästchen **Elemente erstellen** darf markiert sein. Bei den Optionsfeldern muss **Keine** ausgewählt sein.

7. Klicken Sie auf **OK**, um die Konfiguration abzuschließen.

8. Klicken Sie im Microsoft® Exchange-System-Manager mit der rechten Maustaste auf **GFI AntiSpam-Ordner**, und wählen Sie **Alle Aufgaben > Einstellungen weitergeben** aus.

9. Aktivieren Sie das Kontrollkästchen **Ordnerrechte**, und klicken Sie auf **OK**.

Microsoft® Exchange 2007

1. Geben Sie in der **Microsoft® Exchange-Verwaltungsshell** folgenden Befehl ein:

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "Server" -
TopPublicFolder "\'GFI AntiSpam-Ordner'" -User "Default" -Permissions
Contributor
```

Ersetzen Sie „`Server`“ mit dem vollständigen Computernamen.

2. Geben Sie bei Aufforderung `y` ein, um die Berechtigungen für jeden Ordner zu bestätigen.

Dieser Befehl legt als Standardberechtigung für die öffentlichen Ordner von GFI MailEssentials die Teilnehmerrolle fest. Die Benutzer können somit E-Mails in den öffentlichen Ordnern abspeichern, jedoch keine Einträge anzeigen oder ändern. Administratoren haben standardmäßig die Besitzerrolle für die öffentlichen Ordner und können somit Einträge anzeigen und ändern. Weitere Informationen zu Berechtigungen für öffentliche Ordner finden Sie unter:

http://go.gfi.com/?pageid=ME_PFPermissionsExch2007

Microsoft® Exchange 2010

1. Ändern Sie in der Microsoft ® Exchange-Verwaltungsshell den Ordner auf den Microsoft® Exchange-Skriptordner, der sich im Microsoft® Exchange-Installationsordner befindet. Wenn Microsoft® Exchange auf dem Standardpfad installiert wurde, befindet sich der Skriptordner hier:

```
C:\Program Files\Microsoft\Exchange Server\V14\Scripts\
```

2. Geben Sie folgenden Befehl ein:

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "Server" -
TopPublicFolder "\GFI AntiSpam-Ordner" -User "Default" -Permissions
Contributor
```

Ersetzen Sie „`Server`“ mit dem vollständigen Computernamen.

Dieser Befehl legt als Standardberechtigung für die öffentlichen Ordner von GFI MailEssentials die Teilnehmerrolle fest. Die Benutzer können somit E-Mails in den öffentlichen Ordnern abspeichern, jedoch keine Einträge anzeigen oder ändern. Administratoren haben standardmäßig die Besitzerrolle für die öffentlichen Ordner und können somit Einträge anzeigen und ändern. Weitere Informationen zu Berechtigungen für öffentliche Ordner finden Sie unter:

http://go.gfi.com/?pageid=ME_PFPermissionsExch2010

6.8.2 Scannen öffentlicher Ordner verwenden

Überprüfen von Spam-E-Mails

1. Wenn Spam-E-Mails an das Benutzerpostfach zugestellt werden (Posteingang, Junk-Mail-Ordner oder einen benutzerdefinierten Ordner), müssen die einzelnen E-Mail-Benutzer darauf hingewiesen werden, regelmäßig die Spam-E-Mails durchzuschauen.

2. Es kann vorkommen, dass zulässige E-Mails fälschlicherweise als Spam gekennzeichnet wurden (falsch-positive Ergebnisse). Weitere Informationen finden Sie unter „Verwalten zulässiger E-Mails“ (Seite 178).

3. Es kann auch vorkommen, dass Spam-E-Mails nicht erkannt wurden (falsch-negative Ergebnisse). Weitere Informationen finden Sie unter „Verwalten von Spam-E-Mails“ (Seite 179).

Verwalten zulässiger E-Mails

Wie bei jeder Anti-Spam-Lösung dauert es auch bei GFI MailEssentials unter Umständen einige Zeit, bis die optimalen Anti-Spam-Filterbedingungen erreicht sind. Während dieser Zeit kann es vorkommen, dass zulässige E-Mails versehentlich als Spam gekennzeichnet werden.

In solchen Fällen sollten die Benutzer die fälschlicherweise als Spam identifizierten E-Mails in die Ordner **Zur Whitelist hinzufügen** und **Diese E-Mail ist kein Spam** einfügen, um GFI MailEssentials mit der Information zu ‘trainieren’, dass die betreffende E-Mail kein Spam ist.

> **HINWEISE**
>
> 1. In Microsoft® Outlook können E-Mails mittels Drag-and-Drop in den ausgewählten Ordner verschoben werden. Um eine Kopie der E-Mail im Ausgangsordner zu behalten, halten Sie die STRG-Taste gedrückt. Hierdurch wird die E-Mail nur kopiert.
>
> 2. Dieses Handbuch enthält ausführliche Informationen zum Erstellen der GFI AntiSpam-Ordner. Weitere Informationen finden Sie unter „Scannen öffentlicher Ordner aktivieren“ (Seite 174).

Hinzufügen von Absendern zur Whitelist

1. Suchen Sie in der Liste der öffentlichen Ordner des E-Mail-Clients (z. B. Microsoft® Outlook) nach dem öffentlichen Ordner **GFI AntiSpam-Ordner > Zur Whitelist hinzufügen**.

2. Ziehen Sie E-Mails oder Newsletter in den öffentlichen Ordner **Zur Whitelist hinzufügen**.

Hinzufügen von Diskussionslisten zur Whitelist

Bei E-Mails, die an Diskussionslisten gesendet werden, wird die E-Mail-Adresse der Diskussionsliste als Empfänger verwendet. Um E-Mails von bestimmten Diskussionslisten zu erhalten, muss die E-Mail-Adresse der Liste zur Whitelist hinzugefügt werden.

1. Suchen Sie in Ihrem E-Mail-Client (z. B. Microsoft® Outlook) nach dem öffentlichen Ordner **GFI AntiSpam-Ordner > Ich möchte diese Diskussionsliste**.

2. Ziehen Sie Diskussionslisten in den öffentlichen Ordner **Ich möchte diese Diskussionsliste**.

'Trainieren' des Bayes'schen Filters mit zulässigen E-Mails

1. Suchen Sie in den öffentlichen Ordnern des E-Mail-Clients (z. B. Microsoft® Outlook) nach dem öffentlichen Ordner **GFI AntiSpam-Ordner > Diese E-Mail ist kein Spam**.

2. Ziehen Sie E-Mails in den Ordner **Diese E-Mail ist kein Spam**.

Verwalten von Spam-E-Mails

Obwohl GFI MailEssentials von Anfang an standardmäßig Spam-E-Mails identifiziert, kann es vorkommen, dass einzelne Spam-E-Mails unerkannt in das Postfach des Benutzers gelangen. Die Ursache sind meist fehlende Konfigurationseinstellungen oder neue Formen von Spam, an die sich GFI MailEssentials noch nicht angepasst hat. In beiden Fällen lässt sich das Problem beheben, indem GFI MailEssentials für die Erkennung solcher Spam-E-Mails konfiguriert wird.

Die Benutzer sollten die betreffenden E-Mails in den Ordnern **Zur Blocklist hinzufügen** und **Diese E-Mail ist Spam** hinzufügen, um GFI MailEssentials mit der Information zu ‘trainieren’, dass die betreffende E-Mail Spam ist.

> **HINWEISE**
>
> 1. In Microsoft® Outlook können E-Mails mittels Drag-and-Drop in den ausgewählten Ordner verschoben werden. Um eine Kopie der E-Mail im Ausgangsordner zu behalten, halten Sie die STRG-Taste gedrückt. Hierdurch wird die E-Mail nur kopiert.
>
> 2. Dieses Handbuch enthält ausführliche Informationen zum Erstellen der GFI AntiSpam-Ordner. Weitere Informationen finden Sie unter „Scannen öffentlicher Ordner aktivieren“ (Seite 174).

Hinzufügen von Absendern zur E-Mail-Blocklist

1. Suchen Sie in den öffentlichen Ordnern des E-Mail-Clients (z. B. Microsoft® Outlook) nach dem öffentlichen Ordner **GFI AntiSpam-Ordner > Zur Blocklist hinzufügen**.

2. Ziehen Sie E-Mails in den öffentlichen Ordner **Zur Blocklist hinzufügen**.

'Trainieren' des Bayes'schen Filters mit Spam-E-Mails

1. Suchen Sie in den öffentlichen Ordnern des E-Mail-Clients (z. B. Microsoft® Outlook) nach dem öffentlichen Ordner **GFI AntiSpam-Ordner > Diese E-Mail ist Spam**.

2. Ziehen Sie Spam-E-Mails in den Ordner **Diese E-Mail ist Spam**.

7 Inhaltsfilterung

Mit der Inhaltsfilterung können Administratoren den Inhalt von E-Mails kontrollieren. Die Engines scannen den Inhalt von E-Mails und Anhängen und blockieren E-Mails, wenn der Inhalt mit den Inhaltsfilterregeln übereinstimmt.

Themen in diesem Kapitel:

7.1 Stichwortfilterung **180**

7.2 Anhangsfilterung **187**

7.3 Erweiterte Inhaltsfilterung **195**

7.4 Dekomprimierungs-Engine **201**

7.1 Stichwortfilterung

Mithilfe der Stichwortfilterung können Sie Regeln einrichten, um E-Mails auf bestimmte Stichwörter oder Wortgruppen im Text oder Betreff zu filtern. Eine Regel besteht aus folgenden Komponenten:

- Zu blockierende Stichwörter im Text, Betreff oder Anhang von E-Mails
- Aktionen, die bei Erkennung eines Stichworts ausgeführt werden sollen
- Die Benutzer, für die eine Regel gelten soll

Um Inhaltsregeln zu konfigurieren, wählen Sie **Inhaltsfilterung > Stichwortfilterung** aus. Auf dieser Seite können Sie Regeln anzeigen, erstellen, aktivieren, deaktivieren oder löschen.

7.1.1 Erstellen einer Stichwortfilterungsregel

Führen Sie folgende Schritte aus, um eine Regel für die Stichwortfilterung zu erstellen:

- Schritt 1: Konfigurieren der grundlegenden Regeleinstellungen
- Schritt 2: Konfigurieren der Blockierungsbedingungen
- Schritt 3: Konfigurieren der durchzuführenden Aktionen bei erkannten E-Mails
- Schritt 4: Festlegen der Benutzer, für die diese Regel gelten soll

Schritt 1: Konfigurieren der grundlegenden Regeleinstellungen

1. Wählen Sie **Inhaltsfilterung > Stichwortfilterung** aus, und klicken Sie auf **Regel hinzufügen...**
2. Geben Sie im Textfeld **Regelname** einen Namen für die Regel ein.
3. Wählen Sie aus, ob eingehende, ausgehende und/oder interne E-Mails gescannt werden sollen.

Option	Beschreibung
Eingehende E-Mails prüfen	Wählen Sie diese Option aus, um eingehende E-Mails zu scannen.
Ausgehende E-Mails prüfen	Wählen Sie diese Option aus, um ausgehende E-Mails zu scannen.
Interne E-Mails prüfen	Wählen Sie diese Option aus, um interne E-Mails zu scannen. **HINWEIS** Diese Option ist nur verfügbar, wenn GFI MailEssentials auf dem Microsoft® Exchange-Server installiert ist.

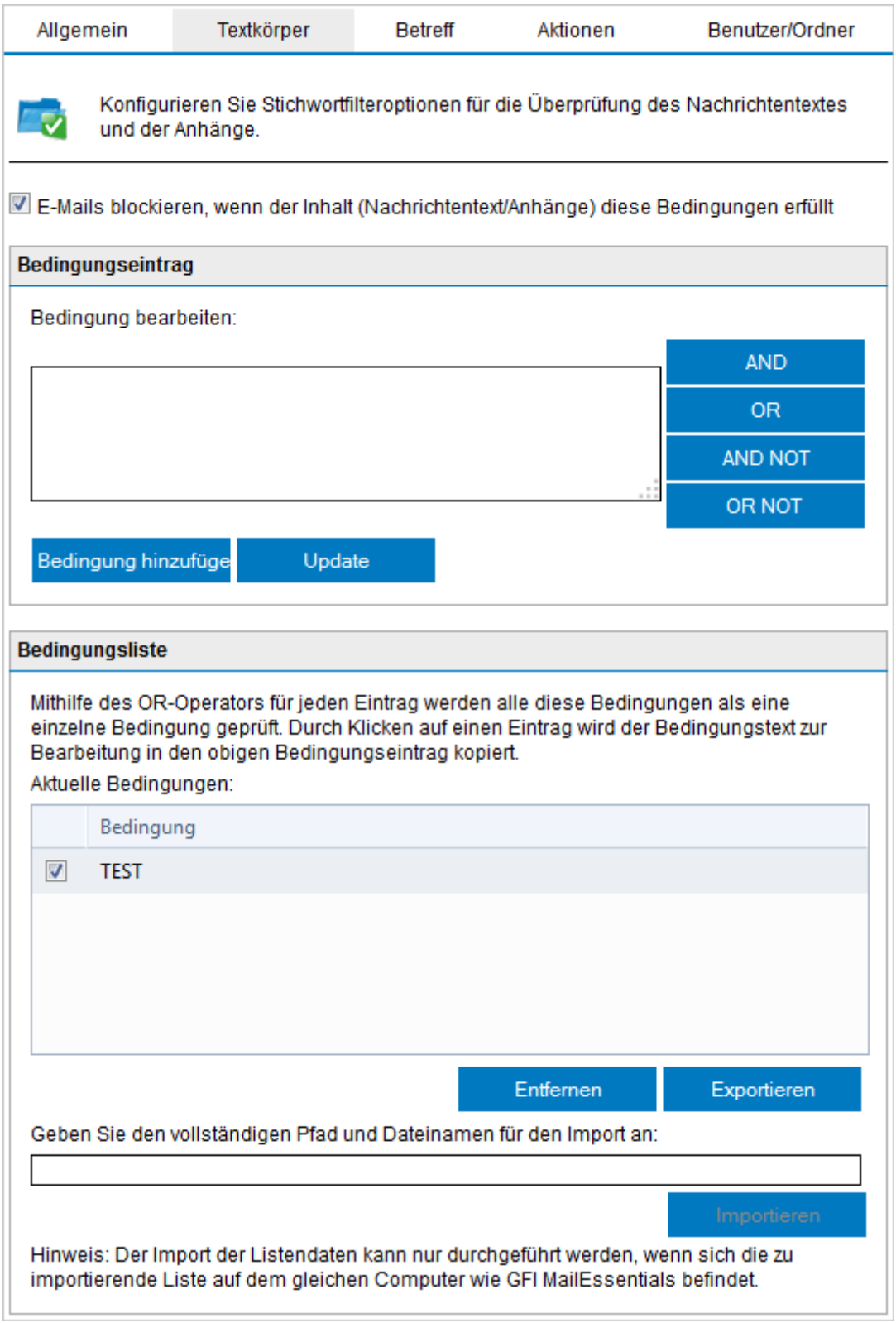
4. Um E-Mails zu blockieren, die mit PGP-Technologie verschlüsselt sind, wählen Sie **PGP-verschlüsselte E-Mail blockieren** aus.

> **HINWEIS**
>
> Die PGP-Verschlüsselung ist ein Kryptosystem mit öffentlichen Schlüsseln, das häufig für E-Mails verwendet wird.

Schritt 2: Konfigurieren der Blockierungsbedingungen

1. Wählen Sie die Registerkarte **Textkörper** aus, um die zu blockierenden Stichwörter im E-Mail-Text anzugeben.

2. Aktivieren Sie das Kontrollkästchen **E-Mails blockieren, wenn der Inhalt diese Bedingungen erfüllt (Nachrichtentext/Anhänge)**, um das Scannen des Texts auf Stichwörter zu aktivieren.


Allgemein
Textkörper
Betreff
Aktionen
Benutzer/Ordner
Konfigurieren Sie Stichwortfilteroptionen für die Überprüfung des Nachrichtentextes und der Anhänge.
E-Mails blockieren, wenn der Inhalt (Nachrichtentext/Anhänge) diese Bedingungen erfüllt
Bedingungseintrag
Bedingung bearbeiten:
AND
OR
AND NOT
OR NOT
Bedingung hinzufüge
Update
Bedingungsliste
Mithilfe des OR-Operators für jeden Eintrag werden alle diese Bedingungen als eine einzelne Bedingung geprüft. Durch Klicken auf einen Eintrag wird der Bedingungstext zur Bearbeitung in den obigen Bedingungseintrag kopiert.
Aktuelle Bedingungen:
Bedingung
TEST
Entfernen
Exportieren
Geben Sie den vollständigen Pfad und Dateinamen für den Import an:
Importieren
Hinweis: Der Import der Listendaten kann nur durchgeführt werden, wenn sich die zu importierende Liste auf dem gleichen Computer wie GFI MailEssentials befindet.

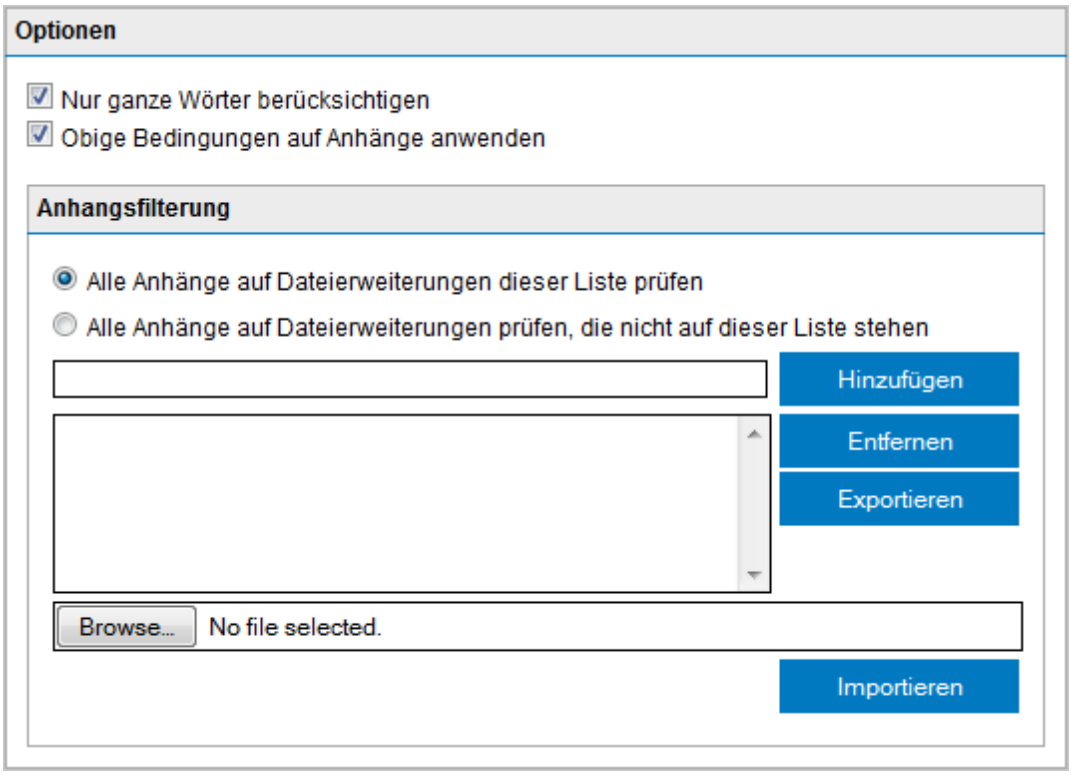
Screenshot 95: Inhaltsfilterung: Registerkarte 'Textkörper' - Bedingungen festlegen

3. Geben Sie im Bereich **Bedingungseintrag** im Feld **Bedingung bearbeiten** Stichwörter ein, die blockiert werden sollen. Sie können auch die Bedingungen **AND**, **OR**, **AND NOT** und **OR NOT** verwenden, um Stichwortkombinationen anzugeben.

4. Zum Hinzufügen des eingegebenen Stichworts oder der Stichwortkombination klicken Sie auf **Bedingung hinzufügen**.

Wählen Sie zum Ändern eines Eintrags diesen in der **Bedingungsliste** aus, und führen Sie die erforderlichen Änderungen im Feld **Bedingungseintrag** durch. Wählen Sie zum Entfernen eines Eintrags diesen aus der **Bedingungsliste** aus, und klicken Sie auf **Entfernen**.

Klicken Sie auf **Aktualisieren**, um die Änderungen zu übernehmen.



Screenshot 96: Inhaltsfilterung: Registerkarte 'Textkörper' - Konfigurieren weiterer Optionen

5. Konfigurieren Sie im Bereich **Optionen** bei Bedarf die folgenden Optionen:

Option	Beschreibung
Nur ganze Wörter berücksichtigen	E-Mails werden blockiert, wenn die festgelegten Stichwörter mit ganzen Wörtern übereinstimmen.
Obige Bedingungen auf Anhänge anwenden	Wählen Sie diese Option aus, um die Regel auch auf Text in Anhängen anzuwenden. Geben Sie im Bereich **Anhangsfilterung** die Dateierweiterung (z. B. `.doc`) für Anhänge ein, für die diese Regel gelten soll bzw. die von der Regel ausgenommen sein sollen.

6. Wählen Sie die Registerkarte **Betreff** aus, um die zu blockierenden Stichwörter für den Betreff anzugeben.

7. Geben Sie im Bereich **Bedingungseintrag** im Feld **Bedingung bearbeiten** Stichwörter ein, die blockiert werden sollen. Sie können auch die Bedingungen **AND**, **OR**, **AND NOT** und **OR NOT** verwenden, um Stichwortkombinationen anzugeben.

8. Zum Hinzufügen des eingegebenen Stichworts oder der Stichwortkombination klicken Sie auf **Bedingung hinzufügen**.

Zum Ändern eines Eintrags in der **Bedingungsliste** wählen Sie ihn aus, und führen Sie die erforderlichen Änderungen im Feld **Bedingungseintrag** durch. Zum Entfernen eines Eintrags aus der **Bedingungsliste** wählen Sie diesen aus, und klicken Sie auf **Entfernen**.

Klicken Sie auf **Aktualisieren**, um die Änderungen zu übernehmen.

9. Konfigurieren Sie im Bereich **Optionen**, wie die Stichwörter verwendet werden sollen. Wählen Sie **Nur ganze Wörter berücksichtigen** aus, um E-Mails nur dann zu blockieren, wenn die festgelegten Stichwörter mit ganzen Wörtern im Betreff übereinstimmen.

Schritt 3: Konfigurieren der durchzuführenden Aktionen bei erkannten E-Mails

1. Konfigurieren Sie auf der Registerkarte **Aktionen**, was geschehen soll, wenn diese Regel ausgelöst wird.

2. Um E-Mails zu blockieren, die den Regelbedingungen entsprechen, wählen Sie **E-Mail blockieren und diese Aktion durchführen** und eine der folgenden Optionen aus:

Option	Beschreibung
E-Mail in Quarantäne verschieben	Speichert blockierte E-Mails im Quarantänespeicher. Danach können Sie alle E-Mails in der Quarantäne überprüfen (zulassen/löschen). Weitere Informationen finden Sie unter „Quarantäne“ (Seite 208).
E-Mail löschen	Löscht blockierte E-Mails.
Verschieben in Ordner auf Festplatte	Verschiebt die E-Mail in einen Ordner auf der Festplatte. Geben Sie den vollständigen Pfad des Ordners ein, in dem blockierte E-Mails gespeichert werden sollen.

WICHTIG

Aktionen betreffen immer die ganze E-Mail, die den blockierten Inhalt aufweist, auch wenn andere Inhalte (z. B. Anhänge) vorhanden sind, die diese Regel nicht auslösen.

HINWEIS

Wenn GFI MailEssentials auf demselben Rechner wie Microsoft® Exchange 2003 installiert wird, kann GFI MailEssentials ausgehende E-Mails möglicherweise nicht blockieren, sondern ersetzt stattdessen den blockierten Inhalt mit einem Bedrohungsbericht.

3. Wählen Sie **Eine bereinigte Kopie der Original-E-Mail an den/die Empfänger senden** aus, wenn eine Kopie der blockierten E-Mail an die Empfänger gesendet werden soll, wobei jedoch der schädliche Inhalt entfernt wurde.

4. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

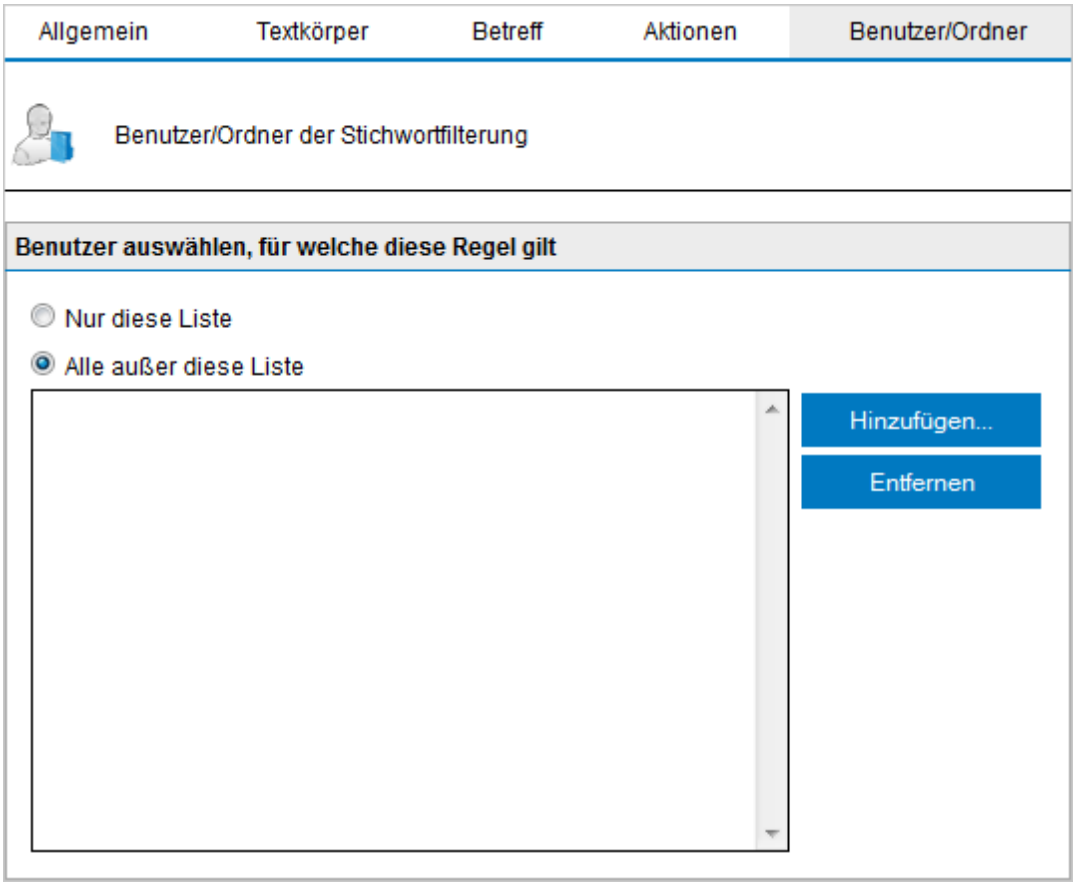
Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

5. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

```
<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log
```

Schritt 4: Festlegen der Benutzer, für die diese Regel gelten soll

1. Die Regel wird standardmäßig auf alle E-Mail-Benutzer angewendet. GFI MailEssentials bietet jedoch die Möglichkeit, die Regel nur auf eine individuelle Liste von E-Mail-Benutzern anzuwenden, die auf der Registerkarte „Benutzer/Ordner“ angegeben werden.

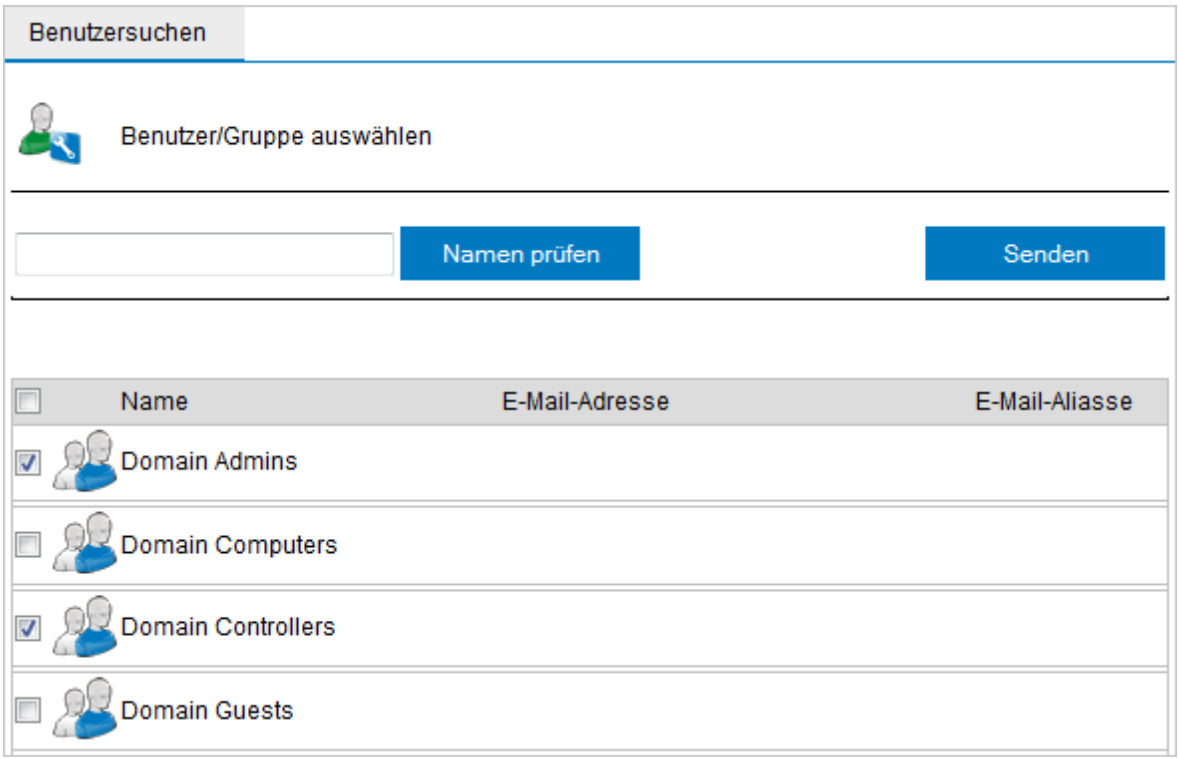


Screenshot 97: Inhaltsfilterung: Registerkarte „Benutzer/Ordner“

2. Geben Sie die Benutzer an, für die diese Regel gelten soll.

Option	Beschreibung
Nur diese Liste	Die Regel gilt für eine individuelle Liste von E-Mail-Benutzern, Gruppen oder öffentlichen Ordnern.
Alle außer diese Liste	Die Regel gilt für alle E-Mail-Benutzer, mit Ausnahme der in der Liste angegebenen E-Mail-Benutzer, Gruppen oder öffentlichen Ordner.

3. Um E-Mail-Benutzer, Benutzergruppen oder öffentliche Ordner zur Liste hinzuzufügen, klicken Sie auf **Hinzufügen**.



Screenshot 98: Hinzufügen von Benutzern zu einer Inhaltsfilterungsregel

4. Geben Sie im Fenster **Benutzersuchen** den Namen des E-Mail-Benutzers, der Benutzergruppe oder des öffentlichen Ordners an, der zur Liste hinzugefügt werden soll, und klicken Sie auf **Namen prüfen**. Die übereinstimmenden Benutzer, Gruppen oder öffentlichen Ordner werden darunter aufgelistet.

> **HINWEIS**
>
> Sie müssen nicht den vollständigen Namen der Benutzer, Gruppen oder öffentlichen Ordner eingeben. Es genügt, wenn Sie einen Teil des Namens eingeben. GFI MailEssentials listet alle Namen auf, die die eingegebene Zeichenfolge enthalten. Wenn Sie beispielsweise `sco` eingeben, gibt GFI MailEssentials Namen wie `Scott Adams` und `Freeman Prescott` zurück, sofern diese verfügbar sind.

5. Aktivieren Sie das Kontrollkästchen neben dem Namen, den Sie der Liste hinzufügen möchten, und klicken Sie auf **OK**.

> **HINWEIS**
>
> Wählen Sie zum Entfernen von Einträgen den betreffenden Benutzer bzw. die Benutzergruppe oder den öffentlichen Ordner in der Liste aus, und klicken Sie auf **Entfernen**.

6. Wiederholen Sie die Schritte 3 bis 5, um alle erforderlichen Benutzer zur Liste hinzuzufügen.

7. Klicken Sie auf **Übernehmen**.

7.1.2 Aktivieren/Deaktivieren von Regeln

So aktivieren/deaktivieren Sie Regeln für die Inhaltsfilterung:

1. Wählen Sie **Inhaltsfilterung > Stichwortfilterung** aus.

2. Wählen Sie auf der Seite **Inhaltsfilterung** die Kontrollkästchen der Regeln aus, die aktiviert oder deaktiviert werden sollen.

3. Klicken Sie nach Bedarf auf **Auswahl aktivieren** oder **Auswahl deaktivieren**.

7.1.3 Entfernen von Regeln für die Inhaltsfilterung

> **WARNHINWEIS**
>
> Gelöschte Regeln können nicht wiederherstellt werden. In Zweifelsfällen wird daher empfohlen, eine Regel nur zu deaktivieren.

1. Wählen Sie **Inhaltsfilterung > Stichwortfilterung** aus.

2. Wählen Sie auf der Inhaltsfilterungsseite die Kontrollkästchen der Regeln aus, die entfernt werden sollen.

3. Klicken Sie auf **Auswahl entfernen**.

7.1.4 Ändern einer vorhandenen Regel

1. Wählen Sie **Inhaltsfilterung > Stichwortfilterung** aus.

2. Klicken Sie auf der Seite **Inhaltsfilterung** auf den Namen der Regel, die geändert werden soll.

3. Führen Sie in den Regeleigenschaften die erforderlichen Änderungen durch, und klicken Sie auf **Übernehmen**.

7.1.5 Ändern der Priorität von Regeln

Regeln für die Inhaltsfilterung werden in der Reihenfolge (von oben nach unten) angewendet, in der sie auf der Inhaltsfilterungsseite angezeigt werden (das heißt, die Regel mit Priorität 1 wird als Erste geprüft). So ändern Sie die Reihenfolge/Priorität von Regeln:

1. Wählen Sie **Inhaltsfilterung > Stichwortfilterung** aus.

2. Klicken Sie auf der Seite **Inhaltsfilterung** auf ↑ (nach oben) oder ↓ (nach unten), um der ausgewählten Regel eine höhere oder niedrigere Priorität zuzuweisen.

3. Wiederholen Sie Schritt 2, bis sich alle Regeln in der gewünschten Reihenfolge befinden.

7.2 Anhangsfilterung

Mithilfe der Anhangsfilterung können Sie Regeln erstellen, um festzulegen, welche E-Mail-Anhangstypen auf dem Mailserver zugelassen oder blockiert werden sollen. Eine Regel besteht aus folgenden Komponenten:

- Anhangtypen, die blockiert werden sollen
- Aktionen, die bei Erkennung eines übereinstimmenden Anhangs ausgeführt werden sollen
- Die Benutzer, für die eine Regel gelten soll

Um Regeln für Anhänge zu konfigurieren, wählen Sie **Inhaltsfilterung > Anhangsfilterung** aus. Auf dieser Seite können Sie Regeln anzeigen, erstellen, aktivieren, deaktivieren oder löschen.

7.2.1 Erstellen einer Regel für die Anhangsfilterung

Führen Sie folgende Schritte aus, um eine Regel für die Anhangsfilterung zu erstellen:

» Schritt 1: Konfigurieren der grundlegenden Regeleinstellungen und Blockierungsbedingungen

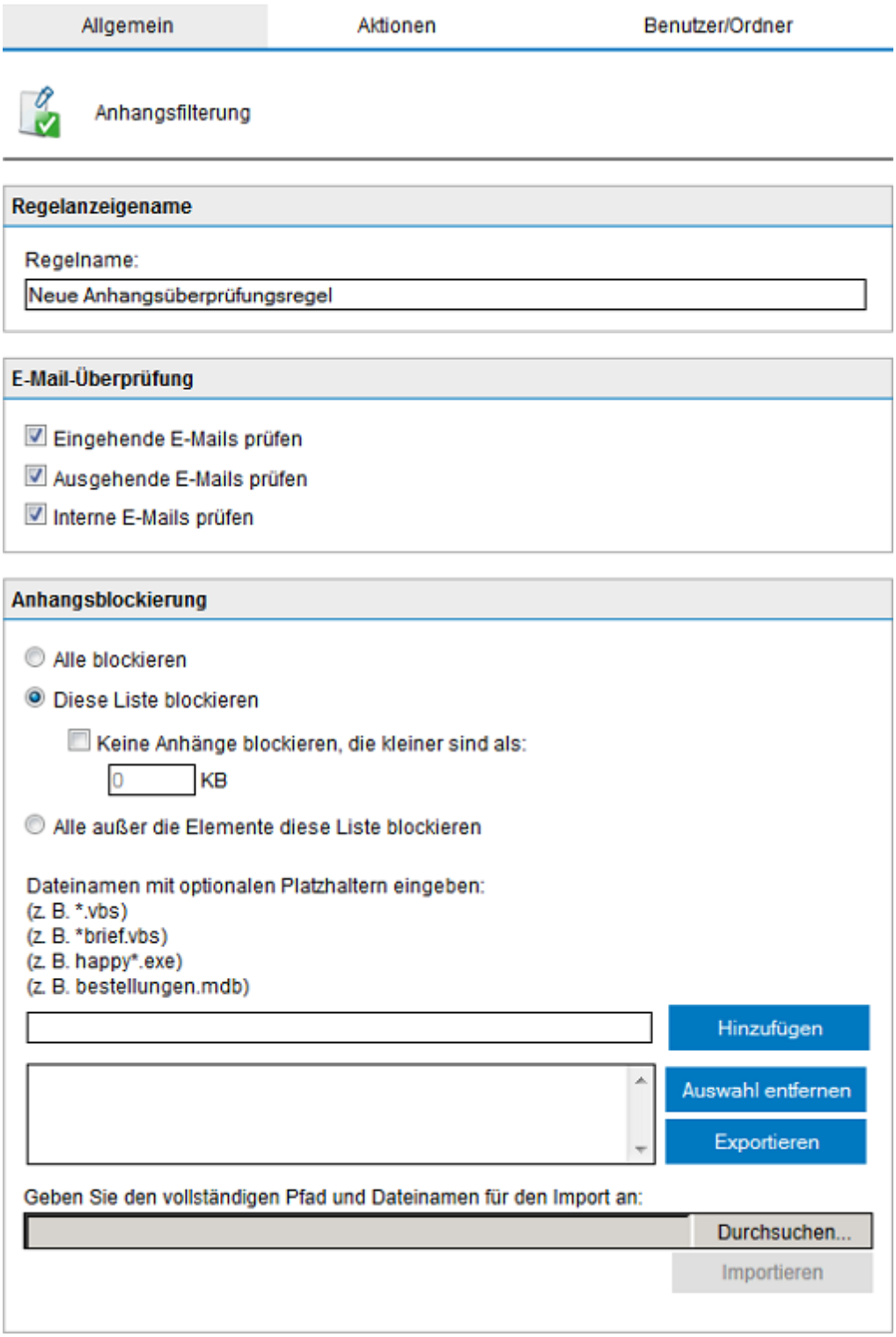
» Schritt 2: Konfigurieren der durchzuführenden Aktionen bei erkannten E-Mails

» Schritt 3: Festlegen der Benutzer, für die diese Regel gelten soll

Schritt 1: Konfigurieren der grundlegenden Regeleinstellungen und Blockierungsbedingungen

1. Wählen Sie **Inhaltsfilterung > Anhangsfilterung** aus.

2. Klicken Sie auf **Regel hinzufügen...**



Screenshot 99: Anhangsfilterung: Registerkarte 'Allgemein'

3. Geben Sie im Textfeld **Regelname** einen Namen für die Regel ein.

4. Wählen Sie aus, ob eingehende, ausgehende und/oder interne E-Mails gescannt werden sollen.

Option	Beschreibung
Eingehende E-Mails prüfen	Wählen Sie diese Option aus, um eingehende E-Mails zu scannen.
Ausgehende E-Mails prüfen	Wählen Sie diese Option aus, um ausgehende E-Mails zu scannen.

Option	Beschreibung
Interne E-Mails prüfen	Wählen Sie diese Option aus, um interne E-Mails zu scannen. **HINWEIS** Diese Option ist nur verfügbar, wenn GFI MailEssentials auf dem Microsoft® Exchange-Server installiert ist.

5. Geben Sie im Bereich **Anhangsblockierung** die Anhangstypen an, die blockiert werden sollen:

Option	Beschreibung
Alle blockieren	Alle E-Mail-Anhänge werden unabhängig vom Typ blockiert.
Diese Liste blockieren	Eine benutzerdefinierte Liste von Anhangstypen wird blockiert. Geben Sie im Textfeld **Dateinamen mit optionalen Platzhaltern eingeben** den Datei- und/oder Anhangstyp ein, der blockiert werden soll, und klicken Sie auf **Hinzufügen**. Wiederholen Sie diesen Schritt für alle Datei- und/oder Anhangstypen, die blockiert werden sollen.
Keine Anhänge blockieren, die kleiner sind als:	Wählen Sie diese Option aus, um Anhangstypen aus der Liste zuzulassen, wenn sie eine bestimmte Größe unterschreiten. Geben Sie die Größe (in KB) im Textfeld ein.
Alle außer die Elemente diese Liste blockieren	Alle Anhänge mit Ausnahme der in der Liste angegebenen Anhänge werden blockiert. Geben Sie im Textfeld **Dateinamen mit optionalen Platzhaltern eingeben** den Datei- und/oder Anhangstyp ein, der zugelassen werden soll, und klicken Sie auf **Hinzufügen**. Wiederholen Sie diesen Schritt für alle Datei- und/oder Anhangstypen, die zugelassen werden sollen.

HINWEIS

Bei der Angabe von Datei- oder Anhangstypen können Sie Sternchen (*) als Platzhalter verwenden. Wenn Sie beispielsweise `*orders*.mdb` eingeben, betrifft dies alle Dateien des Typs **mdb**, die im Dateinamen die Zeichenfolge `orders` enthalten. Wenn Sie `*.jpg` angeben, werden alle Bilder des Typs **jpg** blockiert.

HINWEIS

Wählen Sie zum Entfernen von Einträgen diese aus der Liste aus, und klicken Sie auf **Auswahl entfernen**.

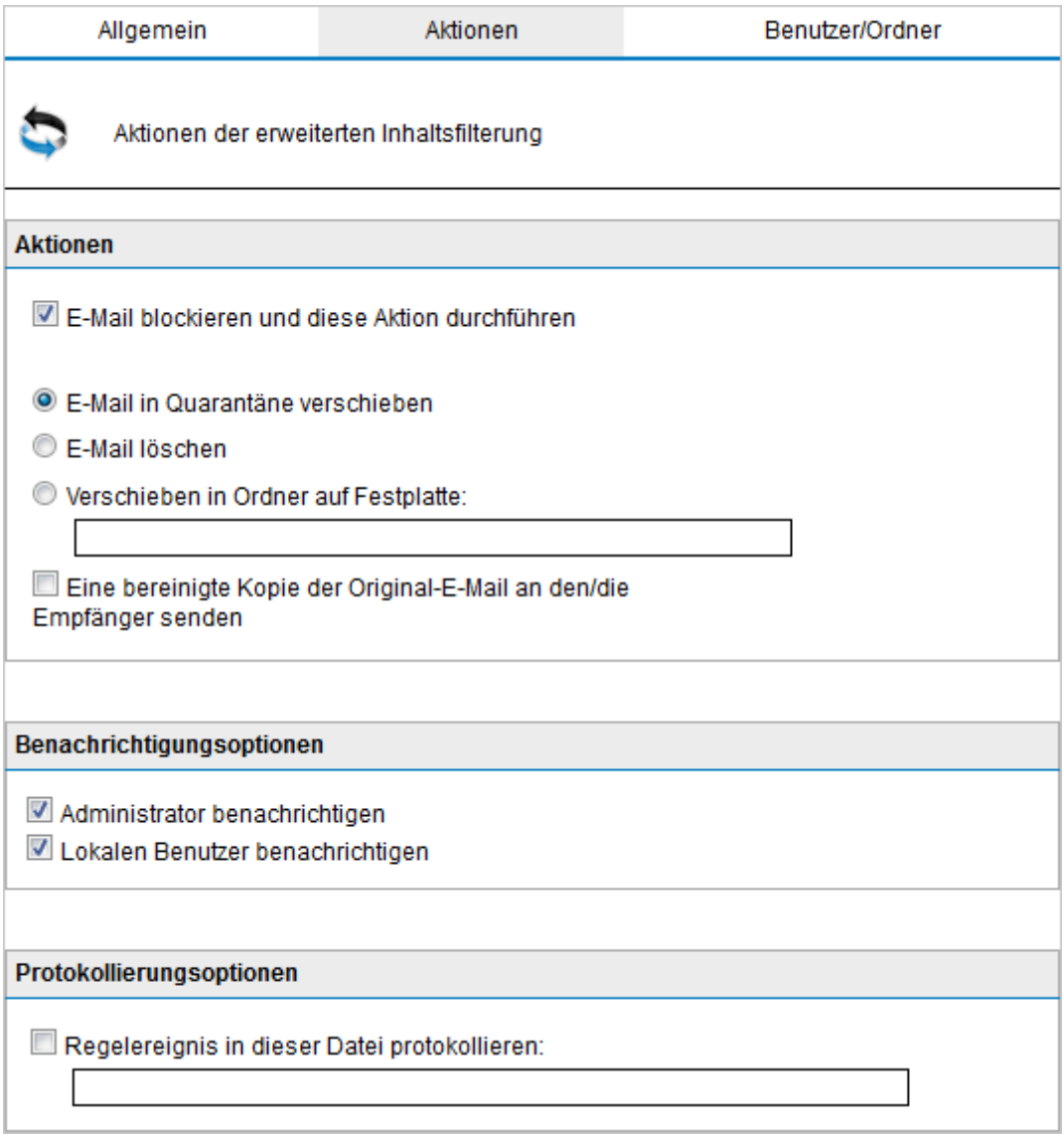
6. Sie können auch Anhänge blockieren, die eine bestimmte Größe überschreiten. Wählen Sie dazu im Bereich **Optionen** die Option **Alle Dateien blockieren, die größer sind als (in KB)** aus, und geben Sie die maximale Anhangsgröße (in KB) ein.

HINWEIS

Mit dieser Funktion werden alle Anhänge blockiert, die größer als die angegebene Dateigröße sind, unabhängig davon, ob sie einem Eintrag in der Liste **Anhangsblockierung** entsprechen.

Schritt 2: Konfigurieren der durchzuführenden Aktionen bei erkannten E-Mails

1. Konfigurieren Sie auf der Registerkarte **Aktionen**, was geschehen soll, wenn diese Regel ausgelöst wird.



Screenshot 100: Anhangsfilterung: Registerkarte für Aktionen

2. Um E-Mails zu blockieren, die den Regelbedingungen entsprechen, wählen Sie **Anhang blockieren und diese Aktion durchführen** und eine der folgenden Optionen aus:

Option	Beschreibung
E-Mail in Quarantäne verschieben	Speichert blockierte E-Mails im Quarantänespeicher. Danach können Sie alle E-Mails in der Quarantäne überprüfen (zulassen/löschen). Weitere Informationen finden Sie unter „Quarantäne“ (Seite 208).
E-Mail löschen	Löscht blockierte E-Mails.
Verschieben in Ordner auf Festplatte	Verschiebt die E-Mail in einen Ordner auf der Festplatte. Geben Sie den vollständigen Pfad des Ordners ein, in dem blockierte E-Mails gespeichert werden sollen.

WICHTIG

Aktionen betreffen immer die ganze E-Mail, die den blockierten Inhalt aufweist, auch wenn andere Inhalte (z. B. Anhänge) vorhanden sind, die diese Regel nicht auslösen.

HINWEIS

Wenn GFI MailEssentials auf demselben Rechner wie Microsoft® Exchange 2003 installiert wird, kann GFI MailEssentials ausgehende E-Mails möglicherweise nicht blockieren, sondern ersetzt stattdessen den blockierten Inhalt mit einem Bedrohungsbericht.

3. Wählen Sie **Eine bereinigte Kopie der Original-E-Mail an den/die Empfänger senden** aus, wenn eine Kopie der blockierten E-Mail an die Empfänger gesendet werden soll, wobei jedoch der schädliche Inhalt entfernt wurde.

4. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

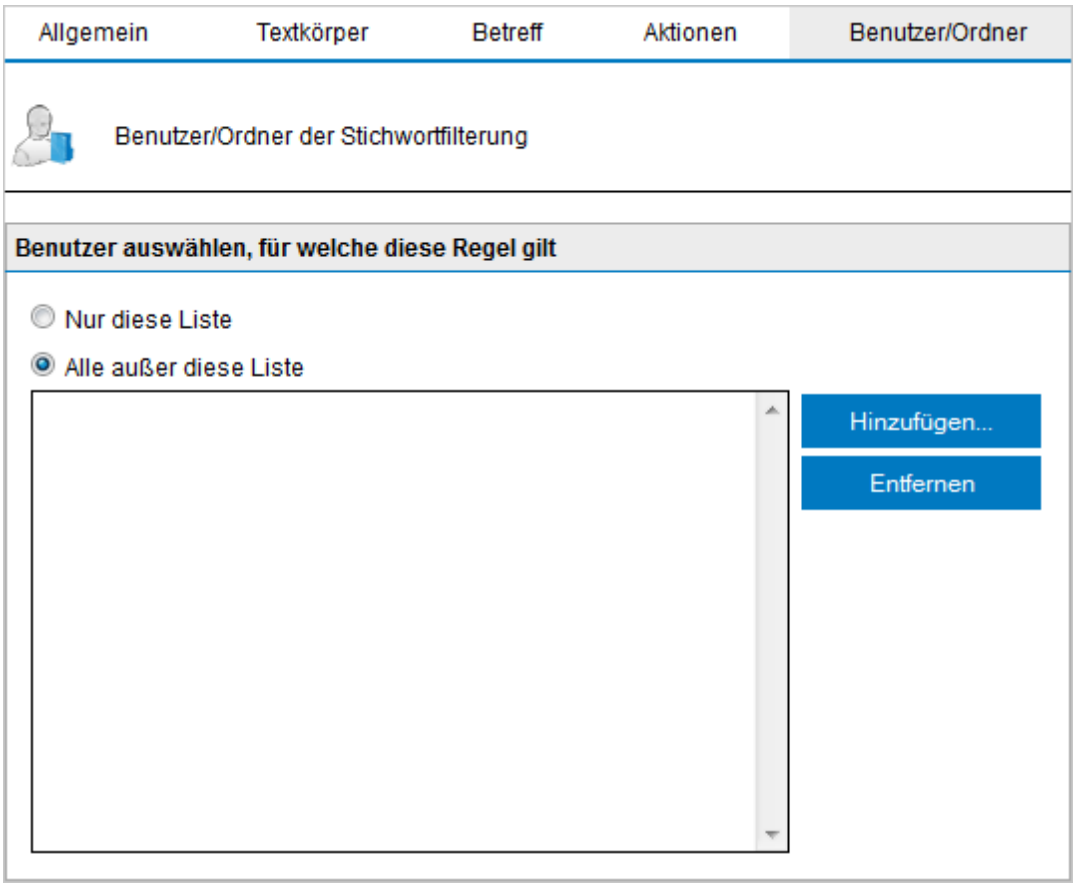
Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

5. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

```
<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log
```

Schritt 3: Festlegen der Benutzer, für die diese Regel gelten soll

1. Die Regel wird standardmäßig auf alle E-Mail-Benutzer angewendet. GFI MailEssentials bietet jedoch die Möglichkeit, die Regel nur auf eine individuelle Liste von E-Mail-Benutzern anzuwenden, die auf der Registerkarte „Benutzer/Ordner“ angegeben werden.

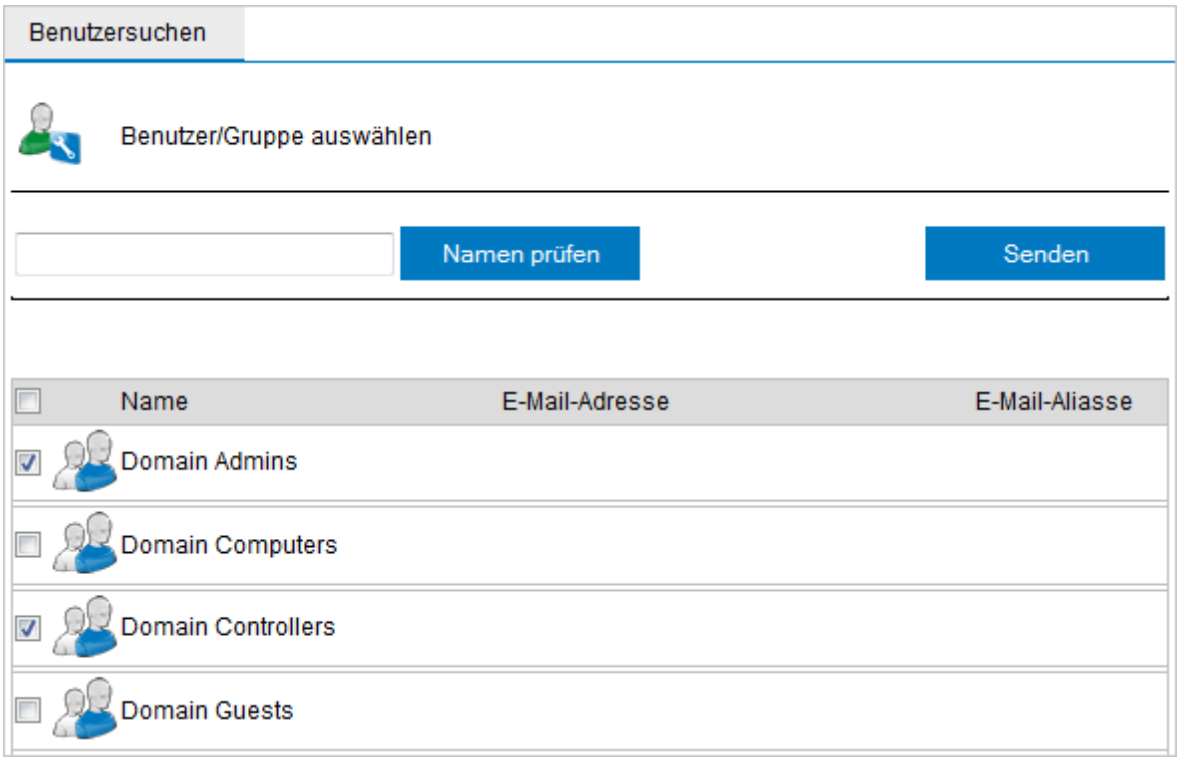


Screenshot 101: Inhaltsfilterung: Registerkarte „Benutzer/Ordner“

2. Geben Sie die Benutzer an, für die diese Regel gelten soll.

Option	Beschreibung
Nur diese Liste	Die Regel gilt für eine individuelle Liste von E-Mail-Benutzern, Gruppen oder öffentlichen Ordnern.
Alle außer diese Liste	Die Regel gilt für alle E-Mail-Benutzer, mit Ausnahme der in der Liste angegebenen E-Mail-Benutzer, Gruppen oder öffentlichen Ordner.

3. Um E-Mail-Benutzer, Benutzergruppen oder öffentliche Ordner zur Liste hinzuzufügen, klicken Sie auf **Hinzufügen**.



Screenshot 102: Hinzufügen von Benutzern zu einer Inhaltsfilterungsregel

4. Geben Sie im Fenster **Benutzersuchen** den Namen des E-Mail-Benutzers, der Benutzergruppe oder des öffentlichen Ordners an, der zur Liste hinzugefügt werden soll, und klicken Sie auf **Namen prüfen**. Die übereinstimmenden Benutzer, Gruppen oder öffentlichen Ordner werden darunter aufgelistet.

> **HINWEIS**
>
> Sie müssen nicht den vollständigen Namen der Benutzer, Gruppen oder öffentlichen Ordner eingeben. Es genügt, wenn Sie einen Teil des Namens eingeben. GFI MailEssentials listet alle Namen auf, die die eingegebene Zeichenfolge enthalten. Wenn Sie beispielsweise `sco` eingeben, gibt GFI MailEssentials Namen wie `Scott Adams` und `Freeman Prescott` zurück, sofern diese verfügbar sind.

5. Aktivieren Sie das Kontrollkästchen neben dem Namen, den Sie der Liste hinzufügen möchten, und klicken Sie auf **OK**.

> **HINWEIS**
>
> Wählen Sie zum Entfernen von Einträgen den betreffenden Benutzer bzw. die Benutzergruppe oder den öffentlichen Ordner in der Liste aus, und klicken Sie auf **Entfernen**.

6. Wiederholen Sie die Schritte 3 bis 5, um alle erforderlichen Benutzer zur Liste hinzuzufügen.

7. Klicken Sie auf **Übernehmen**.

7.2.2 Aktivieren/Deaktivieren von Regeln

So aktivieren oder deaktivieren Sie Regeln für die Anhangsfilterung:

1. Wählen Sie **Inhaltsfilterung > Anhangsfilterung** aus.

2. Wählen Sie auf der Seite **Anhangsfilterung** die Kontrollkästchen der Regeln aus, die aktiviert oder deaktiviert werden sollen.

3. Klicken Sie nach Bedarf auf **Auswahl aktivieren** oder **Auswahl deaktivieren**.

7.2.3 Entfernen von Regeln für Anhänge

> **Warnhinweis**
>
> Gelöschte Regeln können nicht wiederherstellt werden. In Zweifelsfällen wird daher empfohlen, eine Regel nur zu deaktivieren.

1. Wählen Sie **Inhaltsfilterung > Anhangsfilterung** aus.

2. Wählen Sie auf der Seite **Anhangsfilterung** die Regeln aus, die entfernt werden sollen.

3. Klicken Sie auf **Auswahl entfernen**.

7.2.4 Ändern einer vorhandenen Regel

1. Wählen Sie **Inhaltsfilterung > Anhangsfilterung** aus.

2. Klicken Sie auf der Seite **Anhangsfilterung** auf den Namen der Regel, die geändert werden soll.

3. Führen Sie in den Regeleigenschaften die erforderlichen Änderungen durch, und klicken Sie auf **Übernehmen**.

7.2.5 Ändern der Priorität von Regeln

Regeln für die Anhangsfilterung werden in der Reihenfolge (von oben nach unten) ausgeführt, in der sie auf der Seite für die Anhangsfilterung angezeigt werden (das heißt, die Regel mit Priorität 1 wird als Erste geprüft). So ändern Sie die Reihenfolge/Priorität von Regeln:

1. Wählen Sie **Inhaltsfilterung > Anhangsfilterung** aus.

2. Klicken Sie auf der Anhangsfilterungsseite auf ↑ (nach oben) oder ↓ (nach unten), um der ausgewählten Regel eine höhere oder niedrigere Priorität zuzuweisen.

3. Wiederholen Sie Schritt 2, bis sich alle Regeln in der gewünschten Reihenfolge befinden.

7.3 Erweiterte Inhaltsfilterung

Die erweiterte Inhaltsfilterung ermöglicht das Scannen von Inhalten und Header-Daten in E-Mails anhand von konfigurierbaren Suchbedingungen und regulären Ausdrücken (Regex).

Um erweiterte Inhaltsregeln zu konfigurieren, wählen Sie **Inhaltsfilterung > Erweiterte Inhaltsfilterung** aus. Auf dieser Seite können Sie Regeln anzeigen, erstellen, aktivieren, deaktivieren oder löschen.

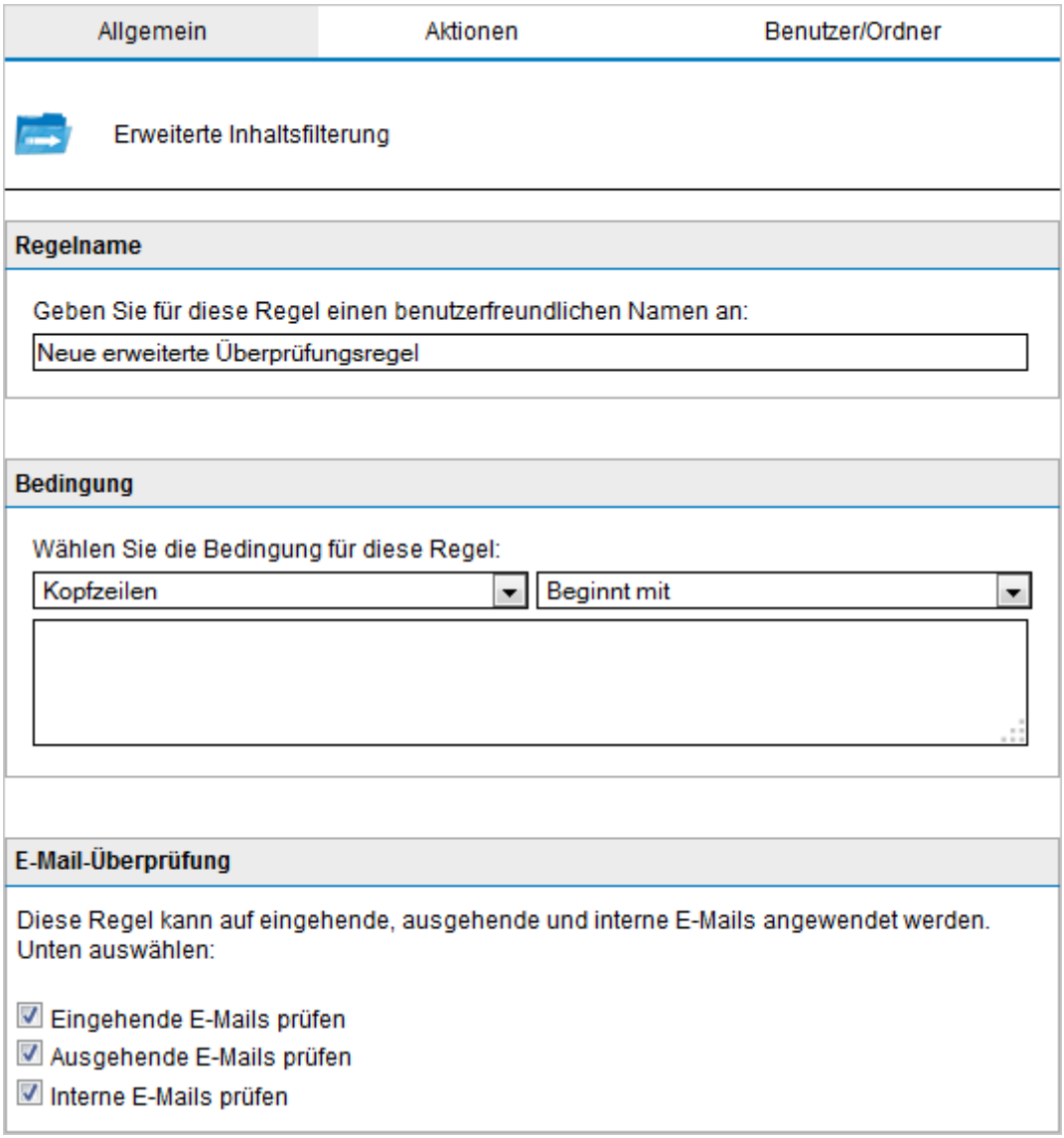
7.3.1 Erstellen von Regeln für die erweiterte Inhaltsfilterung

Führen Sie folgende Schritte aus, um eine Regel für die erweiterte Inhaltsfilterung zu erstellen:

- Schritt 1: Konfigurieren der grundlegenden Regeleinstellungen und Blockierungsbedingungen
- Schritt 2: Konfigurieren der durchzuführenden Aktionen bei erkannten E-Mails
- Schritt 3: Festlegen der Benutzer, für die diese Regel gelten soll

Schritt 1: Konfigurieren der grundlegenden Regeleinstellungen und Blockierungsbedingungen

1. Wählen Sie **Inhaltsfilterung > Erweiterte Inhaltsfilterung** aus, und klicken Sie auf **Regel hinzufügen...**



Screenshot 103: Hinzufügen einer neuen Regel für die erweiterte Inhaltsfilterung

2. Geben Sie im Bereich **Regelname** einen Namen für die neue Regel ein.

3. Geben Sie im Bereich **Bedingung** an, welche Bedingung eine E-Mail erfüllen muss, damit diese Regel zutrifft. Wählen Sie im Dropdown-Menü den E-Mail-Teil aus (**Header**, **Betreff**, **Textkörper**, **Anhangsname** oder **Anhangsinhalt**), und wählen Sie eine Bedingung aus (**Beginnt mit**, **Endet mit**, **Enthält**, **Genaue Übereinstimmung**, **Stimmt mit Regex überein**). Geben Sie im Textfeld das Stichwort oder den regulären Ausdruck ein, mit dem die E-Mail übereinstimmen muss.

> **Beispiel**: Um E-Mails zu filtern, die das Wort `swiss` im Betreff enthalten, wählen Sie **Betreff** und **Enthält** aus, und geben Sie im Textfeld das Wort `swiss` ein.

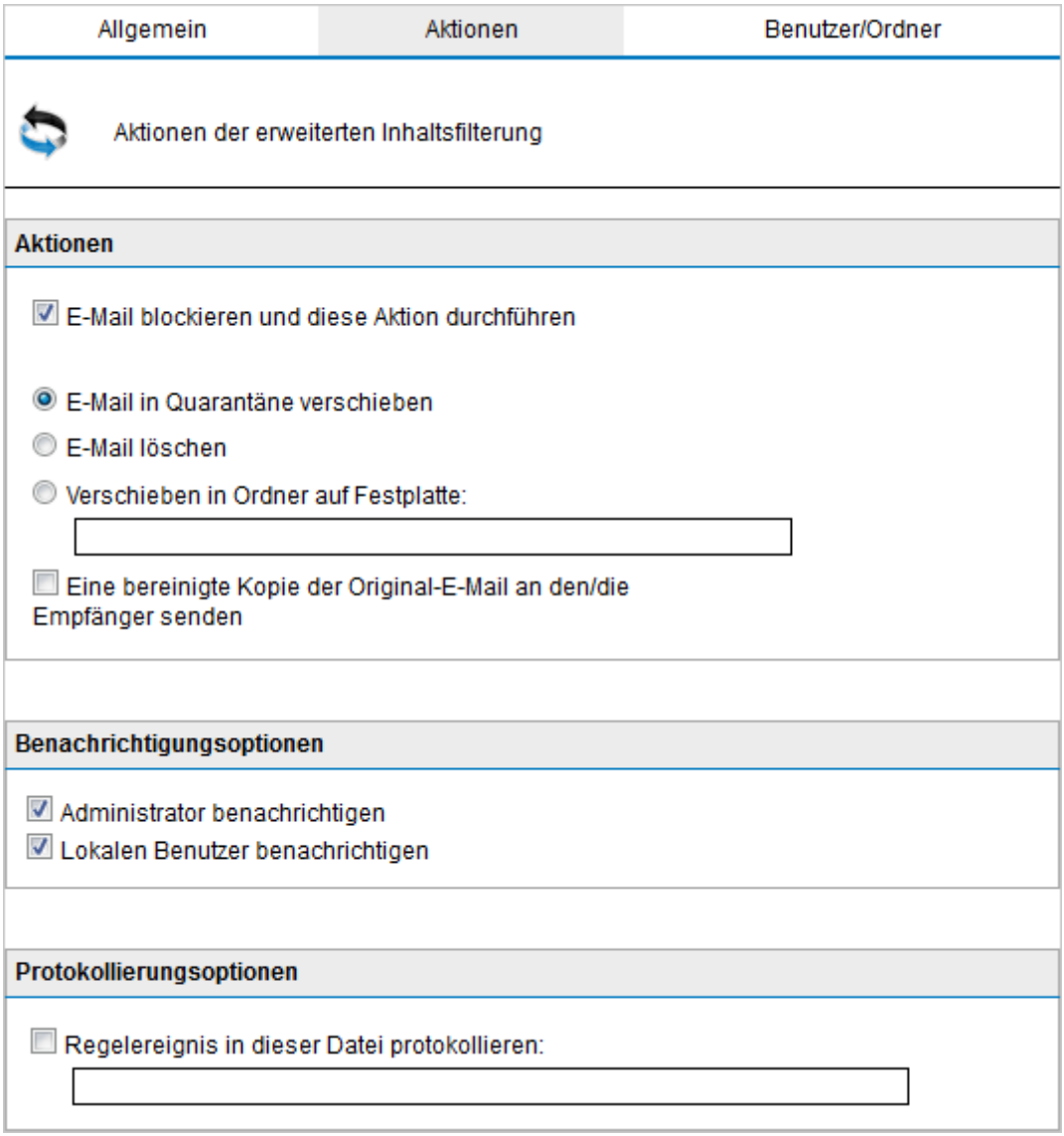
4. Wählen Sie aus, ob eingehende, ausgehende und/oder interne E-Mails gescannt werden sollen.

Option	Beschreibung
Eingehende E-Mails prüfen	Wählen Sie diese Option aus, um eingehende E-Mails zu scannen.

Option	Beschreibung
Ausgehende E-Mails prüfen	Wählen Sie diese Option aus, um ausgehende E-Mails zu scannen.
Interne E-Mails prüfen	Wählen Sie diese Option aus, um interne E-Mails zu scannen. **HINWEIS** Diese Option ist nur verfügbar, wenn GFI MailEssentials auf dem Microsoft® Exchange-Server installiert ist.

Schritt 2: Konfigurieren der durchzuführenden Aktionen bei erkannten E-Mails

1. Konfigurieren Sie auf der Registerkarte **Aktionen**, was geschehen soll, wenn diese Regel ausgelöst wird.



Screenshot 104: Registerkarte für Aktionen

2. Um E-Mails zu blockieren, die den Regelbedingungen entsprechen, wählen Sie **E-Mail blockieren und diese Aktion durchführen** und eine der folgenden Optionen aus:

Option	Beschreibung
E-Mail in Quarantäne verschieben	Speichert blockierte E-Mails im Quarantänespeicher. Danach können Sie alle E-Mails in der Quarantäne überprüfen (zulassen/löschen). Weitere Informationen finden Sie unter „Quarantäne“ (Seite 208).

Option	Beschreibung
E-Mail löschen	Löscht blockierte E-Mails.
Verschieben in Ordner auf Festplatte	Verschiebt die E-Mail in einen Ordner auf der Festplatte. Geben Sie den vollständigen Pfad des Ordners ein, in dem blockierte E-Mails gespeichert werden sollen.

WICHTIG

Aktionen betreffen immer die ganze E-Mail, die den blockierten Inhalt aufweist, auch wenn andere Inhalte (z. B. Anhänge) vorhanden sind, die diese Regel nicht auslösen.

HINWEIS

Wenn GFI MailEssentials auf demselben Rechner wie Microsoft® Exchange 2003 installiert wird, kann GFI MailEssentials ausgehende E-Mails möglicherweise nicht blockieren, sondern ersetzt stattdessen den blockierten Inhalt mit einem Bedrohungsbericht.

3. Wählen Sie **Eine bereinigte Kopie der Original-E-Mail an den/die Empfänger senden** aus, wenn eine Kopie der blockierten E-Mail an die Empfänger gesendet werden soll, wobei jedoch der schädliche Inhalt entfernt wurde.

4. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

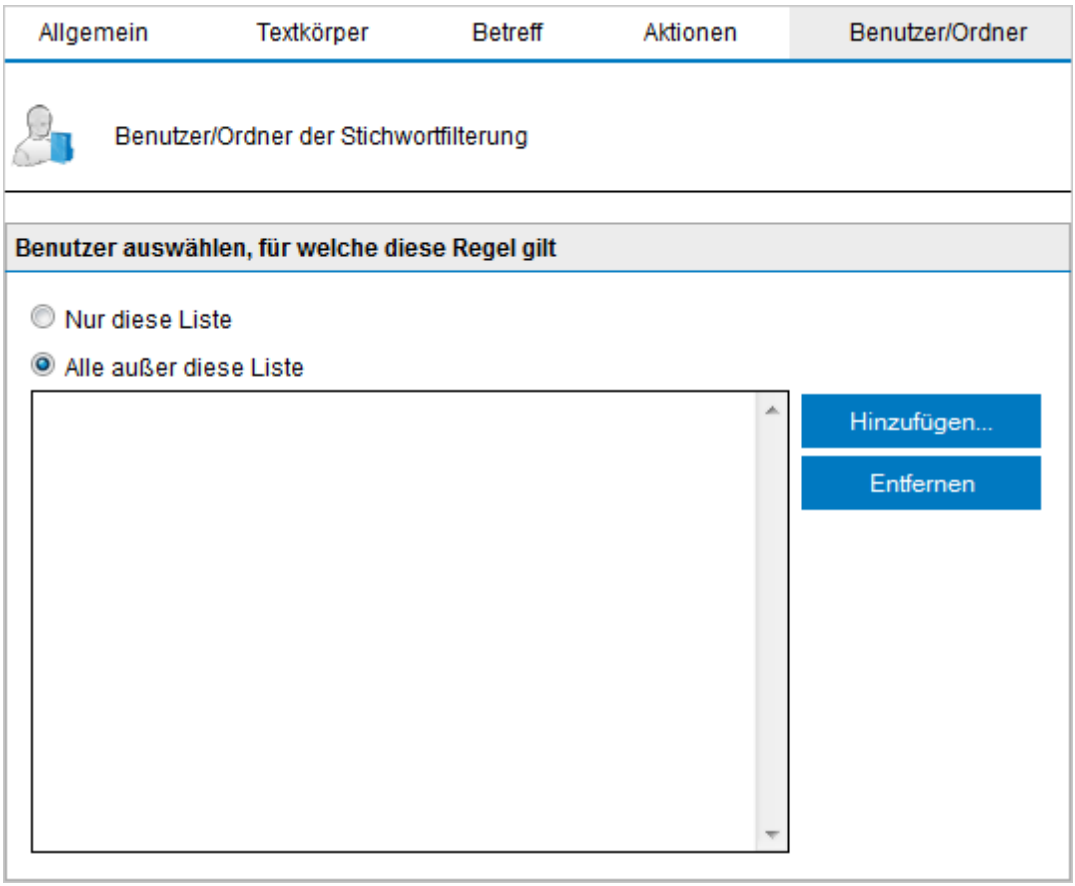
Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

5. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

```
<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log
```

Schritt 3: Festlegen der Benutzer, für die diese Regel gelten soll

1. Die Regel wird standardmäßig auf alle E-Mail-Benutzer angewendet. GFI MailEssentials bietet jedoch die Möglichkeit, die Regel nur auf eine individuelle Liste von E-Mail-Benutzern anzuwenden, die auf der Registerkarte „Benutzer/Ordner“ angegeben werden.

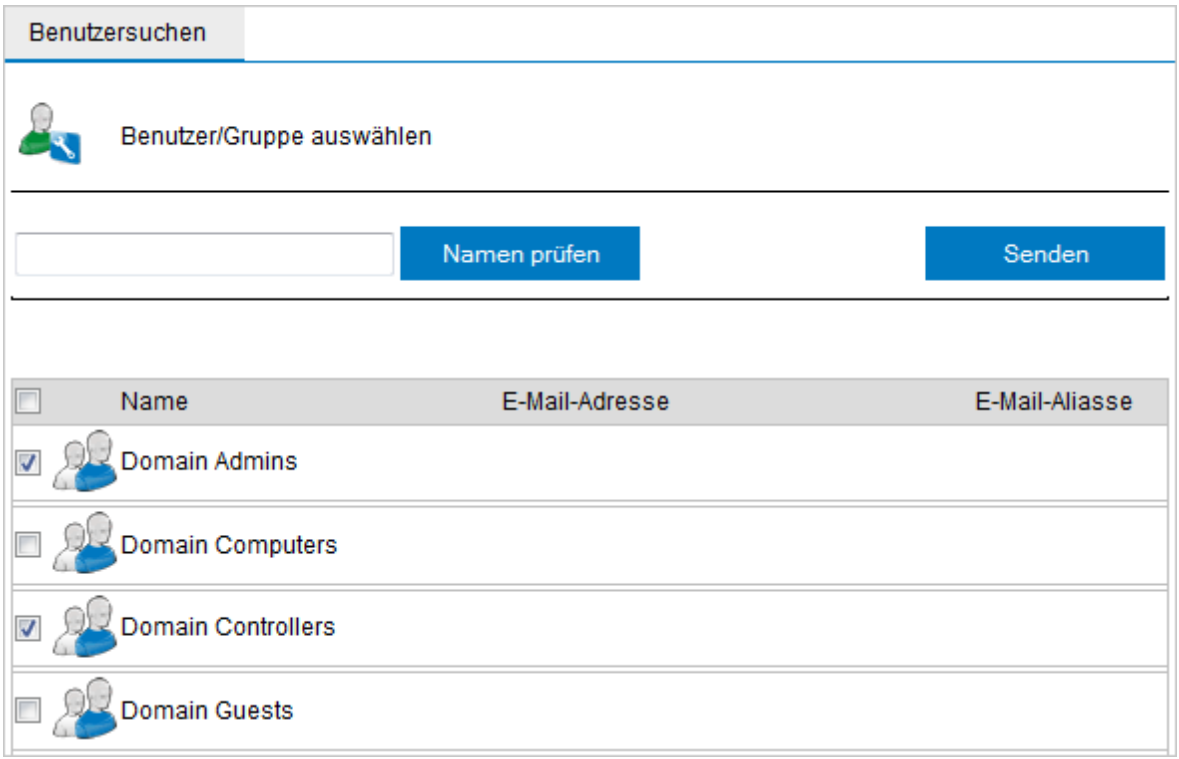


Screenshot 105: Inhaltsfilterung: Registerkarte „Benutzer/Ordner“

2. Geben Sie die Benutzer an, für die diese Regel gelten soll.

Option	Beschreibung
Nur diese Liste	Die Regel gilt für eine individuelle Liste von E-Mail-Benutzern, Gruppen oder öffentlichen Ordnern.
Alle außer diese Liste	Die Regel gilt für alle E-Mail-Benutzer, mit Ausnahme der in der Liste angegebenen E-Mail-Benutzer, Gruppen oder öffentlichen Ordner.

3. Um E-Mail-Benutzer, Benutzergruppen oder öffentliche Ordner zur Liste hinzuzufügen, klicken Sie auf **Hinzufügen**.



Screenshot 106: Hinzufügen von Benutzern zu einer Inhaltsfilterungsregel

4. Geben Sie im Fenster **Benutzersuchen** den Namen des E-Mail-Benutzers, der Benutzergruppe oder des öffentlichen Ordners an, der zur Liste hinzugefügt werden soll, und klicken Sie auf **Namen prüfen**. Die übereinstimmenden Benutzer, Gruppen oder öffentlichen Ordner werden darunter aufgelistet.

> **HINWEIS**
>
> Sie müssen nicht den vollständigen Namen der Benutzer, Gruppen oder öffentlichen Ordner eingeben. Es genügt, wenn Sie einen Teil des Namens eingeben. GFI MailEssentials listet alle Namen auf, die die eingegebene Zeichenfolge enthalten. Wenn Sie beispielsweise `sco` eingeben, gibt GFI MailEssentials Namen wie `Scott Adams` und `Freeman Prescott` zurück, sofern diese verfügbar sind.

5. Aktivieren Sie das Kontrollkästchen neben dem Namen, den Sie der Liste hinzufügen möchten, und klicken Sie auf **OK**.

> **HINWEIS**
>
> Wählen Sie zum Entfernen von Einträgen den betreffenden Benutzer bzw. die Benutzergruppe oder den öffentlichen Ordner in der Liste aus, und klicken Sie auf **Entfernen**.

6. Wiederholen Sie die Schritte 3 bis 5, um alle erforderlichen Benutzer zur Liste hinzuzufügen.

7. Klicken Sie auf **Übernehmen**.

7.3.2 Entfernen von Regeln

1. Wählen Sie unter **Inhaltsfilterung > Erweiterte Inhaltsfilterung** die Regel aus, die entfernt werden soll.

2. Klicken Sie auf **Auswahl entfernen**.

7.3.3 Aktivieren/Deaktivieren von Regeln

1. Wählen Sie unter **Inhaltsfilterung > Erweiterte Inhaltsfilterung** die Regel aus, die aktiviert/deaktiviert werden soll.

2. Klicken Sie auf **Auswahl deaktivieren** oder **Auswahl aktivieren**, um die Regel zu deaktivieren bzw. aktivieren.

7.3.4 Sortieren von Regeln

Regeln für die erweiterte Inhaltsfilterung werden in der Reihenfolge (von oben nach unten) ausgeführt, in der sie auf der Seite für die erweiterte Inhaltsfilterung angezeigt werden (das heißt, die Regel mit Priorität 1 wird als Erste geprüft). So ändern Sie die Reihenfolge/Priorität von Regeln:

1. Wählen Sie **Inhaltsfilterung > Erweiterte Inhaltsfilterung** aus.

2. Klicken Sie auf ↑ (nach oben) oder ↓ (nach unten), um einer Regel eine höhere oder niedrigere Priorität zuzuweisen.

3. Wiederholen Sie Schritt 2, bis sich alle Regeln in der gewünschten Reihenfolge befinden.

7.4 Dekomprimierungs-Engine

Die Dekomprimierungs-Engine extrahiert und analysiert Archive (komprimierte Dateien), die an eine E-Mail angehängt sind.

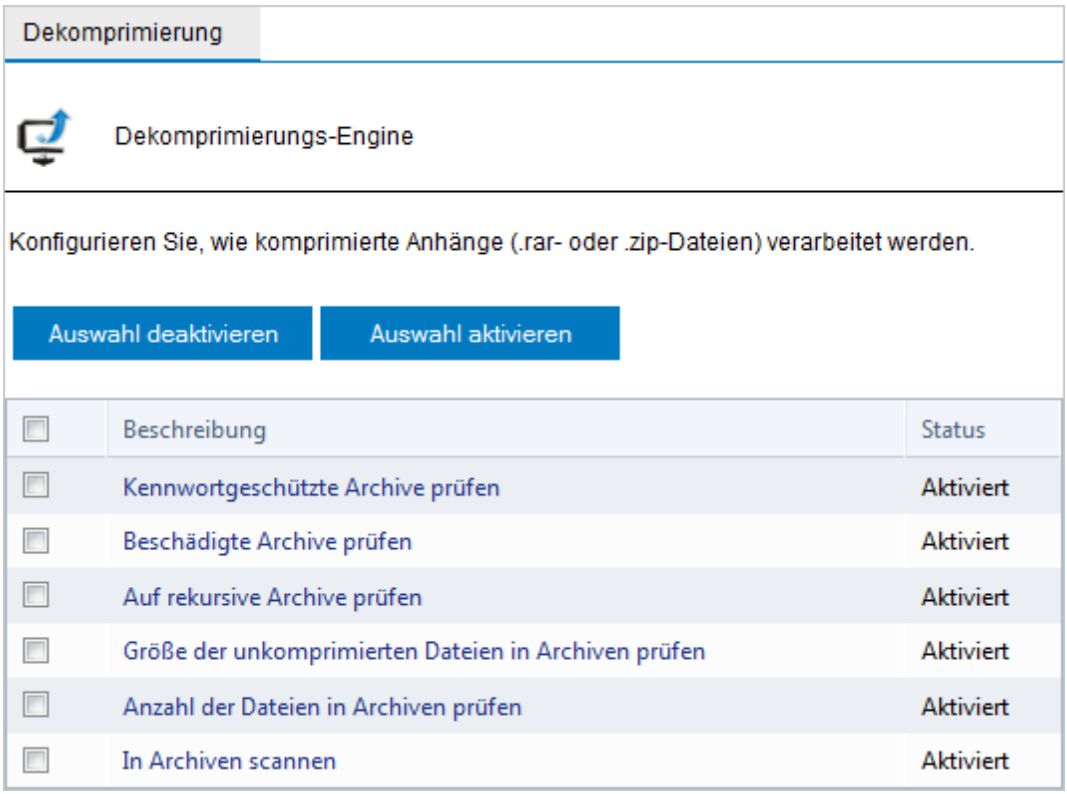
Die Dekomprimierungs-Engine überprüft Folgendes:

- Kennwortgeschützte Archive
- Beschädigte Archive
- Rekursive Archive
- Größe der entpackten Dateien in Archiven
- Anzahl der Dateien in Archiven
- In Archiven scannen

7.4.1 Konfigurieren der Dekomprimierungs-Engine-Filter

So konfigurieren Sie die Filter der Dekomprimierungs-Engine:

1. Wählen Sie **Inhaltsfilterung > Dekomprimierung** aus.



Screenshot 107: Prüfungen durch die Dekomprimierungs-Engine

2. Klicken Sie auf den Dekomprimierungsfilter, den Sie konfigurieren möchten:

» Kennwortgeschützte Archive prüfen

» Beschädigte Archive prüfen

» Auf rekursive Archive prüfen

» Größe der entpackten Dateien in Archiven prüfen

» Anzahl der Dateien in Archiven prüfen

» In Archiven scannen

Kennwortgeschützte Archive prüfen

1. Wählen Sie **Inhaltsfilterung > Dekomprimierung** aus.

2. Klicken Sie in der Liste der verfügbaren Filter auf **Kennwortgeschützte Archive prüfen**.

3. Zum Aktivieren dieses Filters wählen Sie **Kennwortgeschützte Archive prüfen** aus.

4. Geben Sie an, was geschehen soll, wenn eine E-Mail ein Archiv enthält, das diesen Filter auslöst:

Option	Beschreibung
Quarantäne	Verschiebt blockierte E-Mails in die Quarantäne
Automatisch löschen	Löscht blockierte E-Mails

HINWEIS

Wenn GFI MailEssentials auf demselben Rechner wie Microsoft® Exchange 2003 installiert wird, kann GFI MailEssentials ausgehende E-Mails möglicherweise nicht blockieren, sondern ersetzt stattdessen den blockierten Inhalt mit einem Bedrohungsbericht.

5. Wählen Sie **Eine bereinigte Kopie der Original-E-Mail an den/die Empfänger senden** aus, wenn eine Kopie der blockierten E-Mail an die Empfänger gesendet werden soll.

6. Klicken Sie auf die Registerkarte **Aktionen**, um weitere Aktionen zu konfigurieren.

7. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

8. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

```
<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log
```

9. Klicken Sie auf **Übernehmen**.

Beschädigte Archive prüfen

1. Wählen Sie **Inhaltsfilterung > Dekomprimierung** aus.

2. Klicken Sie in der Liste der verfügbaren Filter auf **Beschädigte Archive prüfen**.

3. Zum Aktivieren dieses Filters wählen Sie **Beschädigte Archive prüfen** aus.

4. Geben Sie an, was geschehen soll, wenn eine E-Mail ein Archiv enthält, das diesen Filter auslöst:

Option	Beschreibung
Quarantäne	Verschiebt blockierte E-Mails in die Quarantäne
Automatisch löschen	Löscht blockierte E-Mails

> **HINWEIS**
>
> Wenn GFI MailEssentials auf demselben Rechner wie Microsoft® Exchange 2003 installiert wird, kann GFI MailEssentials ausgehende E-Mails möglicherweise nicht blockieren, sondern ersetzt stattdessen den blockierten Inhalt mit einem Bedrohungsbericht.

5. Wählen Sie **Eine bereinigte Kopie der Original-E-Mail an den/die Empfänger senden** aus, wenn eine Kopie der blockierten E-Mail an die Empfänger gesendet werden soll.

6. Klicken Sie auf die Registerkarte **Aktionen**, um weitere Aktionen zu konfigurieren.

7. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

8. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

```
<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log
```

9. Klicken Sie auf **Übernehmen**.

Auf rekursive Archive prüfen

Mit diesem Filter können Sie E-Mails, die rekursive Archive enthalten, in die Quarantäne verschieben oder löschen. Rekursive Archive (verschachtelte Archive) sind Archive, die mehrere Ebenen von Unterarchiven (Archive innerhalb von Archiven) enthalten. Eine hohe Anzahl an Archivebenen kann ein Hinweis auf ein schädliches Archiv sein. Rekursive Archive können für DoS-Angriffe (Denial of Service) verwendet werden, da sie bei ihrer Analyse Rechnerressourcen verbrauchen. So konfigurieren Sie diesen Filter:

1. Wählen Sie **Inhaltsfilterung > Dekomprimierung** aus.

2. Klicken Sie in der Liste der verfügbaren Filter auf **Auf rekursive Archive prüfen**.

3. Zum Aktivieren dieses Filters wählen Sie **Auf rekursive Archive prüfen** aus.

4. Legen Sie die maximale Anzahl rekursiver Archive im Textfeld **Maximale Anzahl von wiederkehrenden Archiven** fest. Enthält ein Archiv eine höhere Anzahl rekursiver Archive, wird die E-Mail als schädlich klassifiziert.

5. Geben Sie an, was geschehen soll, wenn eine E-Mail ein Archiv enthält, das diesen Filter auslöst:

Option	Beschreibung
Quarantäne	Verschiebt blockierte E-Mails in die Quarantäne
Automatisch löschen	Löscht blockierte E-Mails

> **HINWEIS**
>
> Wenn GFI MailEssentials auf demselben Rechner wie Microsoft® Exchange 2003 installiert wird, kann GFI MailEssentials ausgehende E-Mails möglicherweise nicht blockieren, sondern ersetzt stattdessen den blockierten Inhalt mit einem Bedrohungsbericht.

6. Wählen Sie **Eine bereinigte Kopie der Original-E-Mail an den/die Empfänger senden** aus, wenn eine Kopie der blockierten E-Mail an die Empfänger gesendet werden soll, wobei jedoch der schädliche Inhalt entfernt wurde.

7. Klicken Sie auf die Registerkarte **Aktionen**, um weitere Aktionen zu konfigurieren.

8. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

9. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

```
<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log
```

10. Klicken Sie auf **Übernehmen**.

Größe der unkomprimierten Dateien in Archiven prüfen

Mit diesem Filter können Sie E-Mails mit Archiven blockieren oder löschen, die nach dem Entpacken eine bestimmte physische Größe überschreiten. Hacker versenden für DoS-Angriffe (Denial of Service) manchmal ein Archiv, das beim Entpacken eine sehr große Datei enthält. Diese verbraucht Festplattenspeicher, und ihre Analyse durch Content Security- oder Anti-Virus-Software ist sehr zeitaufwändig.

So konfigurieren Sie diesen Filter:

1. Wählen Sie **Inhaltsfilterung > Dekomprimierung** aus.

2. Klicken Sie in der Liste der verfügbaren Filter auf **Größe der unkomprimierten Dateien in Archiven prüfen**.

3. Zum Aktivieren dieses Filters, wählen Sie **Größe der unkomprimierten Dateien in Archiven prüfen** aus.

4. Legen Sie die maximale Größe für dekomprimierte Archive in Textfeld **Maximale Größe der unkomprimierten Dateien im Archiv [in MB]** fest. Ist ein dekomprimiertes Archiv größer als der angegebene Wert, wird die E-Mail als schädlich klassifiziert.

5. Geben Sie an, was geschehen soll, wenn eine E-Mail ein Archiv enthält, das diesen Filter auslöst:

Option	Beschreibung
Quarantäne	Verschiebt blockierte E-Mails in die Quarantäne
Automatisch löschen	Löscht blockierte E-Mails

> **HINWEIS**
>
> Wenn GFI MailEssentials auf demselben Rechner wie Microsoft® Exchange 2003 installiert wird, kann GFI MailEssentials ausgehende E-Mails möglicherweise nicht blockieren, sondern ersetzt stattdessen den blockierten Inhalt mit einem Bedrohungsbericht.

6. Wählen Sie **Eine bereinigte Kopie der Original-E-Mail an den/die Empfänger senden** aus, wenn eine Kopie der blockierten E-Mail an die Empfänger gesendet werden soll, wobei jedoch der schädliche Inhalt entfernt wurde.

7. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

8. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll. Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

```
<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log
```

9. Klicken Sie auf **Übernehmen**.

Anzahl der Dateien in Archiven prüfen

Mit diesem Filter können Sie E-Mails, die eine sehr hohe Anzahl an komprimierten Dateien in einem angehängten Archiv enthalten, in die Quarantäne verschieben oder löschen. Über die Konfigurationsoptionen dieses Filters können Sie festlegen, wie viele Dateien in einem Archivanhang zulässig sein sollen. So konfigurieren Sie diesen Filter:

1. Wählen Sie **Inhaltsfilterung > Dekomprimierung** aus.

2. Klicken Sie in der Liste der verfügbaren Filter auf **Anzahl der Dateien in Archiven prüfen**.

3. Zum Aktivieren dieses Filters wählen Sie **Anzahl der Dateien in Archiven prüfen** aus.

4. Legen Sie die maximale Anzahl an Dateien für Archive im Textfeld **Wenn die Dateianzahl im Archiv folgenden Wert überschreitet** fest. Enthält ein Archiv mehr Dateien, wird die E-Mail als schädlich klassifiziert.

5. Geben Sie an, was geschehen soll, wenn eine E-Mail ein Archiv enthält, das diesen Filter auslöst:

Option	Beschreibung
Quarantäne	Verschiebt blockierte E-Mails in die Quarantäne
Automatisch löschen	Löscht blockierte E-Mails

> **HINWEIS**
>
> Wenn GFI MailEssentials auf demselben Rechner wie Microsoft® Exchange 2003 installiert wird, kann GFI MailEssentials ausgehende E-Mails möglicherweise nicht blockieren, sondern ersetzt stattdessen den blockierten Inhalt mit einem Bedrohungsbericht.

6. Wählen Sie **Eine bereinigte Kopie der Original-E-Mail an den/die Empfänger senden** aus, wenn eine Kopie der blockierten E-Mail an die Empfänger gesendet werden soll.

7. Klicken Sie auf die Registerkarte **Aktionen**, um weitere Aktionen zu konfigurieren.

8. GFI MailEssentials kann eine Benachrichtigung senden, wenn eine E-Mail diesen Filter auslöst. Wählen Sie nach Bedarf die folgenden Optionen aus, um diese Funktion zu aktivieren:

Option	Beschreibung
Administrator benachrichtigen	Der Administrator wird benachrichtigt, wenn diese Engine eine E-Mail blockiert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).
Lokalen Benutzer benachrichtigen	Die lokalen E-Mail-Empfänger werden über die blockierte E-Mail benachrichtigt.

9. Um die Aktivitäten dieser Engine in einer Protokolldatei zu speichern, wählen Sie **Ereignis in dieser Datei protokollieren** aus. Geben Sie im Textfeld den Pfad und Dateinamen eines benutzerdefinierten Speicherorts auf der Festplatte an, unter dem die Protokolldatei gespeichert werden soll.

Standardmäßig werden Protokolldateien im folgenden Verzeichnis gespeichert:

<GFI MailEssentials Installationspfad>\GFI\MailEssentials\EmailSecurity\Logs\<Name der Engine>.log

10. Klicken Sie auf **Übernehmen**.

In Archiven scannen

Sie können GFI MailEssentials so konfigurieren, dass eine Stichwort- und Anhangsfilterung für Dateien in Archiven durchgeführt wird.

1. Wählen Sie **Inhaltsfilterung > Dekomprimierung** aus.

2. Klicken Sie in der Liste der verfügbaren Filter auf **In Archiven scannen**.

3. Zum Aktivieren des Scans für Archive wählen Sie **Anhangs- und Inhaltsfilterungsregeln in Archiven anwenden** aus. Weitere Informationen finden Sie unter „Inhaltsfilterung“ (Seite 180).

4. Klicken Sie auf **Übernehmen**.

7.4.2 Aktivieren/Deaktivieren von Dekomprimierungsfiltern

So aktivieren oder deaktivieren Sie Dekomprimierungsfilter:

1. Wählen Sie **Inhaltsfilterung > Dekomprimierung** aus.

2. Wählen Sie auf der Seite **Dekomprimierungs-Engine** die Kontrollkästchen der Filter aus, die aktiviert oder deaktiviert werden sollen.

3. Klicken Sie nach Bedarf auf **Auswahl aktivieren** oder **Auswahl deaktivieren**.

8 Quarantäne

Die Quarantäne von GFI MailEssentials ist ein zentraler Speicher, wo alle als Spam oder Malware erkannten E-Mails verbleiben. Dies stellt sicher, dass die Benutzer in ihrem Postfach keine Spam- oder Malware-Nachrichten empfangen, und die für die Verarbeitung dieser E-Mails verwendeten Ressourcen auf dem Mailserver werden reduziert.

Administratoren und E-Mail-Benutzer können die E-Mails in Quarantäne anzeigen, indem Sie mit einem Webbrowser auf die Quarantäneoberfläche zugreifen. GFI MailEssentials kann außerdem reguläre E-Mail-Berichte an E-Mail-Benutzer senden, um über die blockierten E-Mails zu informieren.

Weitere Informationen zum Konfigurieren der Quarantäne von GFI MailEssentials finden Sie in den folgenden Abschnitten.

8.1 Wichtige Hinweise **208**

8.2 Durchsuchen der Quarantäne **208**

8.3 Suchordner **214**

8.4 Arbeiten mit E-Mails in Quarantäne **217**

8.5 Quarantäne-RSS-Feeds **221**

8.6 Quarantäneoptionen **223**

8.7 Speicherort des Quarantänespeichers und öffentliche URL **229**

8.1 Wichtige Hinweise

1. Um Spam-Nachrichten oder schädliche E-Mails unter Quarantäne zu stellen, ändern Sie die Aktionen der Filter und Engines auf **E-Mail in Quarantäne verschieben**.

2. Der Quarantänespeicher benötigt Festplattenspeicher, um die Spam- oder Malware-E-Mails des Unternehmens für einige Tage aufzubewahren. Der erforderliche Festplattenspeicher hängt von Folgendem ab:

- Menge der empfangenen Nachrichten
- Zeitdauer, für die Nachrichten aufbewahrt werden sollen

3. Durchschnittlich benötigen 100.000 Spam- oder Malware-E-Mails mit einer Größe von jeweils 5 KB einschließlich der Metadaten etwa 600 MB Festplattenspeicher.

4. Wenn der freie Festplattenspeicher am Speicherort des Quarantänespeichers gleich oder kleiner als 512 MB ist, stoppt GFI MailEssentials das Verschieben von Spam- und Malware-E-Mails in die Quarantäne. Diese werden stattdessen gekennzeichnet und in die Empfängerpostfächer zugestellt, bis der freie Festplattenspeicher wieder größer als 512 MB ist. Das stellt sicher, dass die Festplatte nicht voll wird.

8.2 Durchsuchen der Quarantäne

Der Quarantänespeicher ist über die GFI MailEssentials-Oberfläche zugänglich und ermöglicht die Verwaltung von E-Mails in Quarantäne.

Zum Öffnen des Quarantänespeichers von GFI MailEssentials wählen Sie **GFI MailEssentials > Quarantäne** aus.

Es gibt verschiedene Möglichkeiten, in der GFI MailEssentials-Quarantäne nach Inhalten zu suchen:

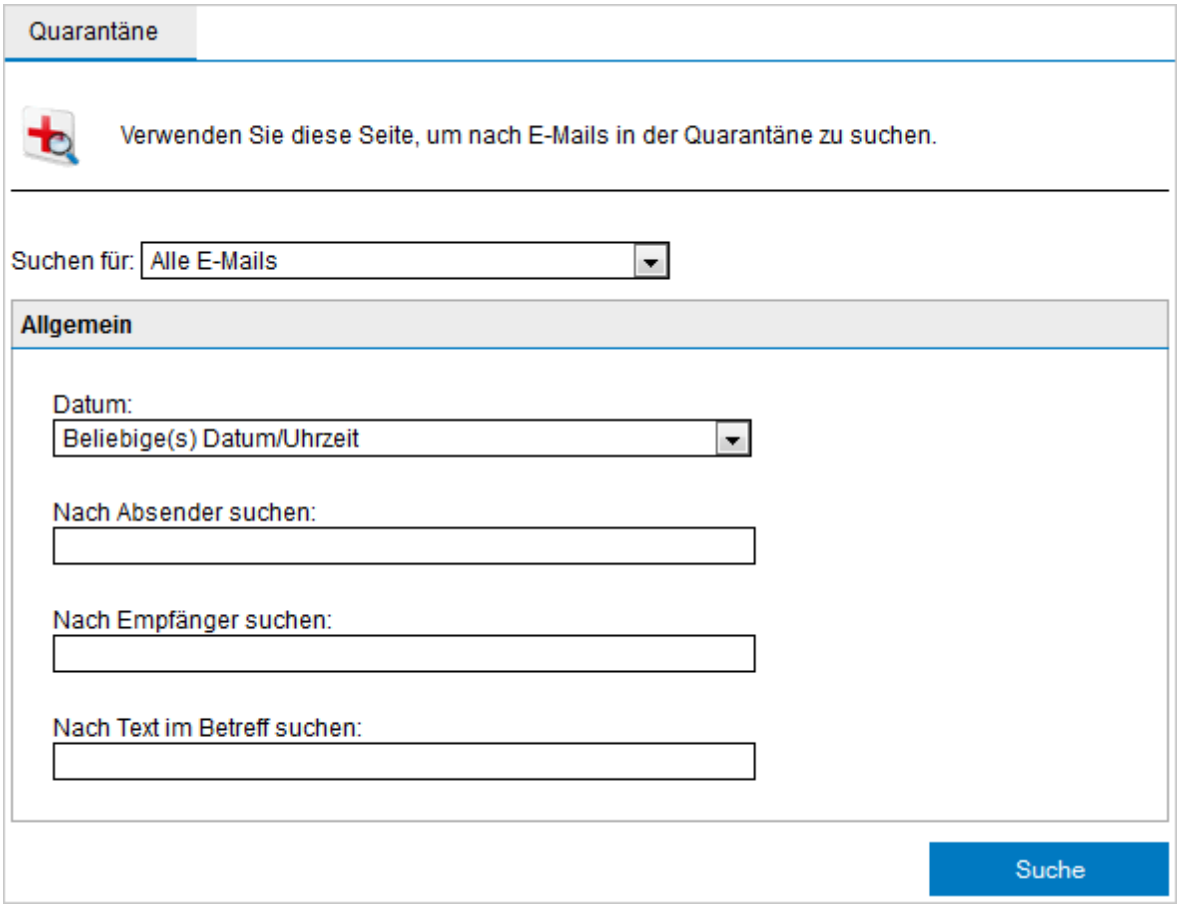
» Malware- und Spam-E-Mails in der Quarantäne durchsuchen

» Nur Malware-E-Mails durchsuchen

» Nur Spam-E-Mails durchsuchen

Malware- und Spam-E-Mails durchsuchen

1. Wählen Sie **GFI MailEssentials > Quarantäne** aus.



Screenshot 108: Suchbereich für Malware- und Spam-E-Mails

2. Wählen Sie auf der Seite **Quarantäne** in der Dropdown-Liste **Suchen nach** die Option **Alle E-Mails** aus.

3. Geben Sie die erforderlichen Suchkriterien an.

SUCHKRITERIEN	BESCHREIBUNG
Datum:	Wählen Sie den Datumsbereich aus, in dem die E-Mail in die Quarantäne verschoben wurde. Folgende Datumsbereiche stehen zur Auswahl: » Beliebige(s) Datum/Uhrzeit » Seit gestern » Letzte 7 Tage » Letzte 30 Tage » Benutzerdefinierter Datumsbereich
Nach Absender suchen	Geben Sie den Absender der gesuchten E-Mail in der Quarantäne an.
Nach Empfänger suchen	Geben Sie den Empfänger der gesuchten E-Mail in der Quarantäne an.

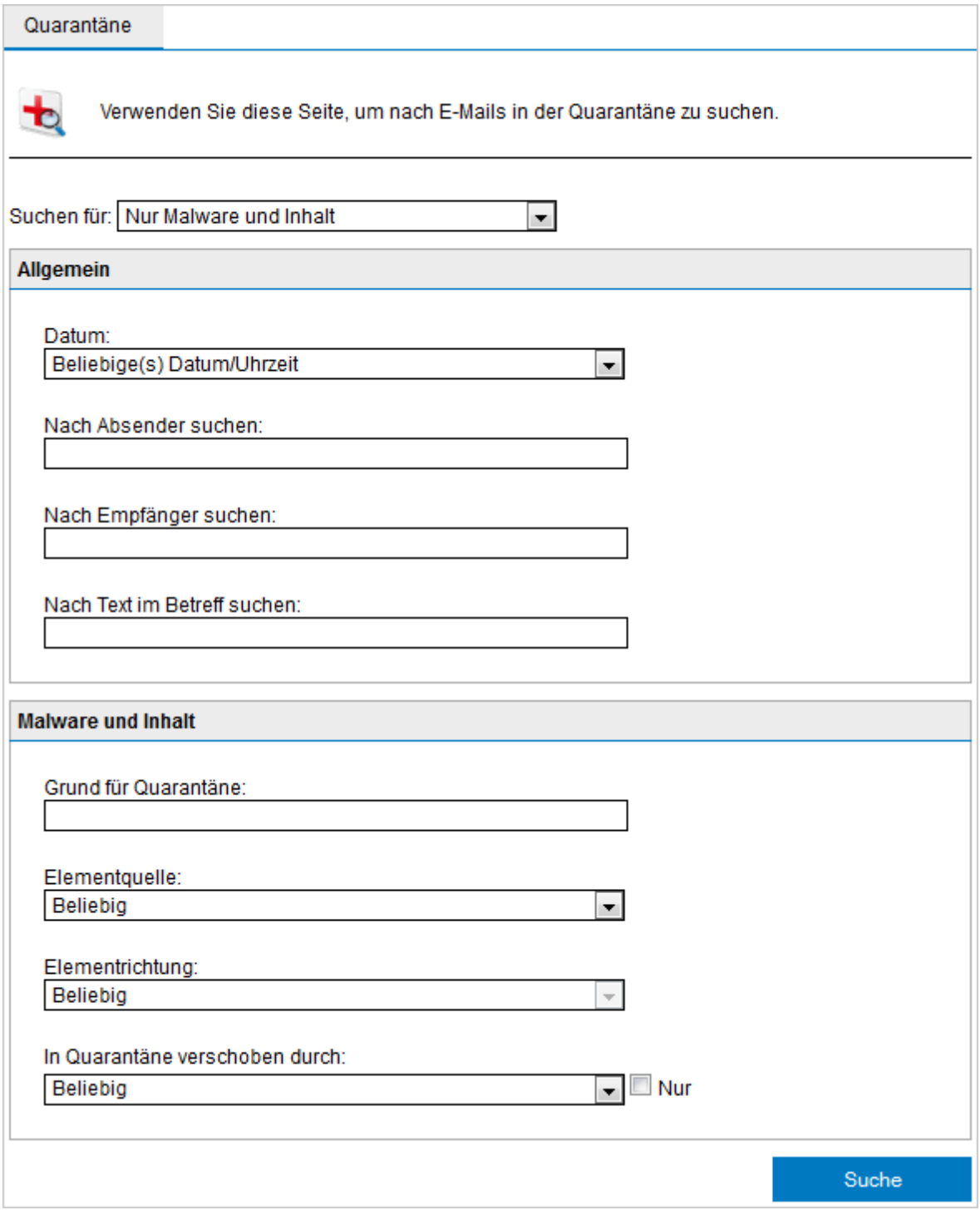
SUCHKRITERIEN	BESCHREIBUNG
Nach Text im Betreff suchen	Geben Sie den Text ein, der im Betreff von E-Mails in der Quarantäne gesucht werden soll.

4. Klicken Sie auf **Suchen**.

> **HINWEIS**
>
> Überprüfen Sie die E-Mails in Quarantäne anhand der Suchergebnisse. Falsch-positive Ergebnisse können zur Zustellung an die Empfänger bestätigt werden. Weitere Informationen finden Sie unter „Arbeiten mit E-Mails in Quarantäne“ (Seite 217).

Nur Malware- und Inhaltsfilter-E-Mails durchsuchen

1. Wählen Sie **GFI MailEssentials > Quarantäne** aus.



Screenshot 109: Suchbereich für Malware- und Spam-E-Mails

2. Wählen Sie auf der Seite **Quarantäne** in der Dropdown-Liste **Suchen nach** die Option **Nur Malware und Inhalt** aus.

3. Geben Sie die erforderlichen Suchkriterien an.

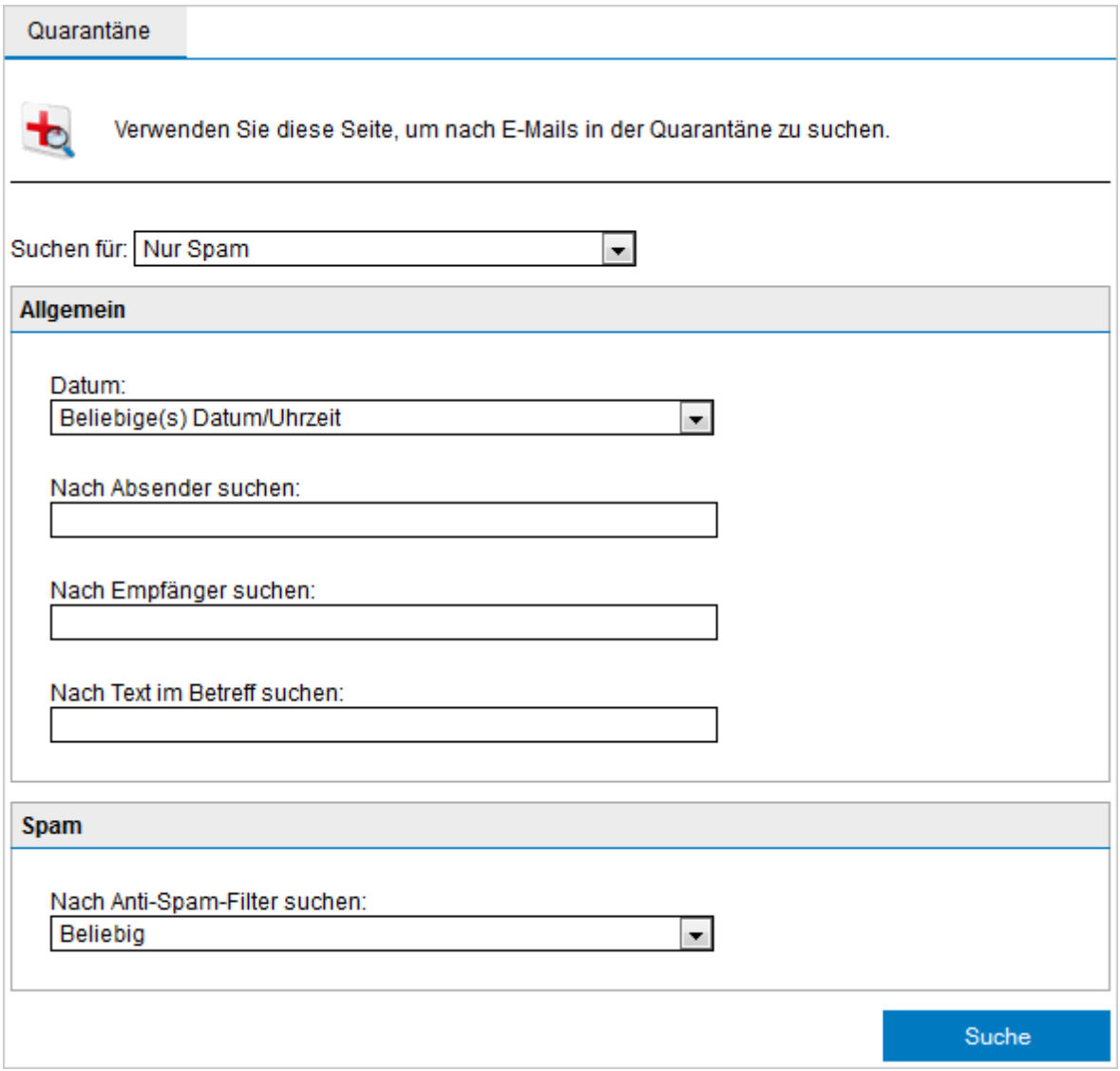
SUCHKRITERIEN	BESCHREIBUNG
Datum:	Wählen Sie den Datumsbereich aus, in dem die E-Mail in die Quarantäne verschoben wurde. Folgende Datumsbereiche stehen zur Auswahl: » Beliebige(s) Datum/Uhrzeit » Seit gestern » Letzte 7 Tage » Letzte 30 Tage » Benutzerdefinierter Datumsbereich
Nach Absender suchen	Geben Sie den Absender der gesuchten E-Mail in der Quarantäne an.
Nach Empfänger suchen	Geben Sie den Empfänger der gesuchten E-Mail in der Quarantäne an.
Nach Text im Betreff suchen	Geben Sie den Text ein, der im Betreff von E-Mails in der Quarantäne gesucht werden soll.
Grund für Quarantäne	Geben Sie an, warum die gesuchte E-Mail in die Quarantäne verschoben wurde.
Elementquelle	Wählen Sie die Quelle aus, in der die E-Mail als Malware identifiziert und in die Quarantäne verschoben wurde. Folgende Optionen sind verfügbar: » Informationsspeicher (VSAPI) » Gateway (SMTP) » Informationsspeicher (Transport)
Elementrichtung	Wählen Sie die Richtung der gesuchten E-Mail in der Quarantäne aus. » Beliebig » Eingehend » Ausgehend **HINWEIS** Diese Option ist nur verfügbar, wenn **Gateway (SMTP)** als **Elementquelle** ausgewählt ist.
In Quarantäne verschoben durch	Wählen Sie den GFI MailEssentials-Filter aus, durch den die E-Mail in die Quarantäne verschoben wurde. Aktivieren Sie das Kontrollkästchen **Nur**, um nur nach E-Mails zu suchen, die von einem bestimmten Filter in die Quarantäne verschoben wurden.

4. Klicken Sie auf **Suchen**.

> **HINWEIS**
>
> Überprüfen Sie die E-Mails in Quarantäne anhand der Suchergebnisse. Falsch-positive Ergebnisse können zur Zustellung an die Empfänger bestätigt werden. Weitere Informationen finden Sie unter „Arbeiten mit E-Mails in Quarantäne“ (Seite 217).

Nur Spam-E-Mails durchsuchen

1. Wählen Sie **GFI MailEssentials > Quarantäne** aus.



Screenshot 110: Nur-Spam-Suchbereich

2. Wählen Sie auf der Seite **Quarantäne** in der Dropdown-Liste **Suchen nach** die Option **Nur Spam** aus.

3. Geben Sie die erforderlichen Suchkriterien an. Folgende Optionen sind verfügbar:

SUCHKRITERIEN	BESCHREIBUNG
Datum:	Wählen Sie den Datumsbereich aus, in dem die E-Mail in die Quarantäne verschoben wurde. Folgende Datumsbereiche stehen zur Auswahl: » Beliebige(s) Datum/Uhrzeit » Seit gestern » Letzte 7 Tage » Letzte 30 Tage » Benutzerdefinierter Datumsbereich
Nach Absender suchen	Geben Sie den Absender der gesuchten E-Mail in der Quarantäne an.
Nach Empfänger suchen	Geben Sie den Empfänger der gesuchten E-Mail in der Quarantäne an.
Nach Text im Betreff suchen	Geben Sie den Text ein, der im Betreff von E-Mails in der Quarantäne gesucht werden soll.

SUCHKRITERIEN	BESCHREIBUNG
Nach Anti-Spam-Filter suchen	Wählen Sie den Anti-Spam-Filter aus, der die gesuchte E-Mail als Spam identifiziert hat.

4. Klicken Sie auf **Suchen**.

> **HINWEIS**
>
> Überprüfen Sie die E-Mails in Quarantäne anhand der Suchergebnisse. Falsch-positive Ergebnisse können zur Zustellung an die Empfänger bestätigt werden. Weitere Informationen finden Sie unter „Arbeiten mit E-Mails in Quarantäne“ (Seite 217).

8.3 Suchordner

Ein Suchordner ist ein Ordner, dem eine benutzerdefinierte Suchabfrage zugewiesen ist und der alle E-Mails in der Quarantäne anzeigt, die dieser Suchabfrage entsprechen.

Beispiele für Suchordner:

» Ein Suchordner, der nur ausgehende E-Mails anzeigt, die von den Virenscan-Engines unter Quarantäne gestellt wurden

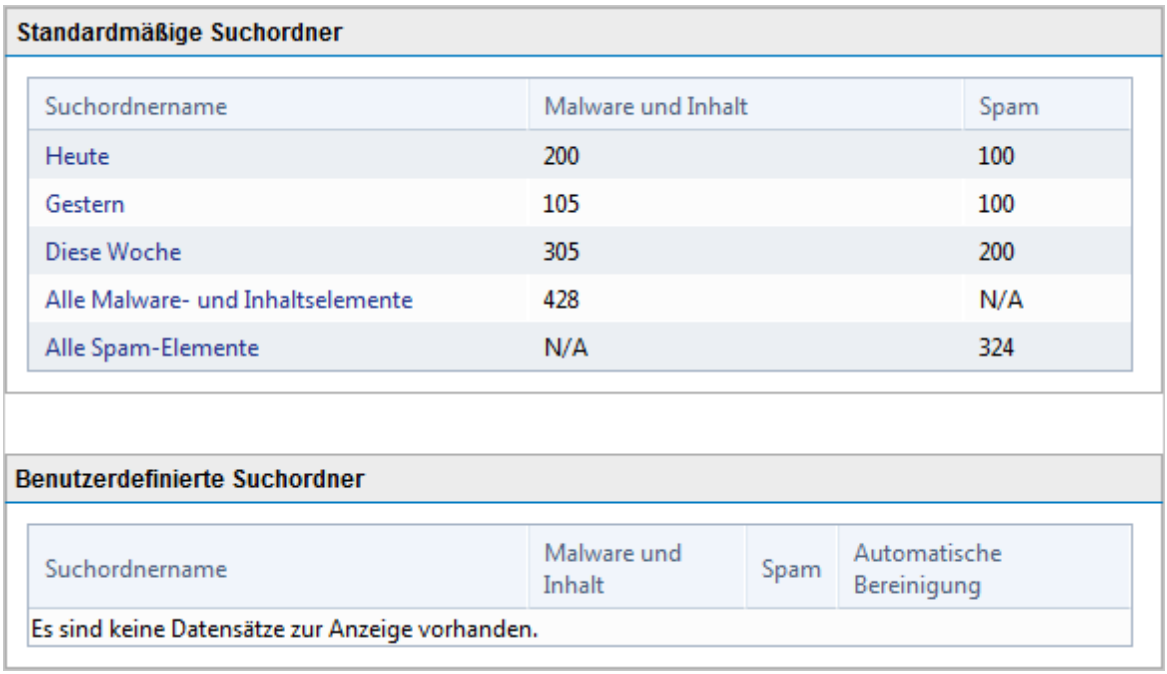
» Ein Suchordner für eingehende E-Mails, die innerhalb eines bestimmten Datumsbereichs in die Quarantäne gestellt wurden und an einen bestimmten Benutzer adressiert sind

» Ein Suchordner, der E-Mails anzeigt, die bestimmten Suchkriterien entsprechen

» Ein Suchordner, der die Ergebnisse einer zuvor definierten Suchabfrage anzeigt

So zeigen Sie die E-Mails in einem bestimmten Suchordner an:

1. Wählen Sie den Knoten **Quarantäne** aus.



Screenshot 111: Standardmäßige und benutzerdefinierte Suchordner

2. Klicken Sie im Bereich **Standardmäßige Suchordner** oder **Benutzerdefinierte Suchordner** auf einen Suchordner. Sie können auch einen der Suchordnerknoten im Knoten **Quarantäne** oder **Quarantäne > Suchordner** auswählen.

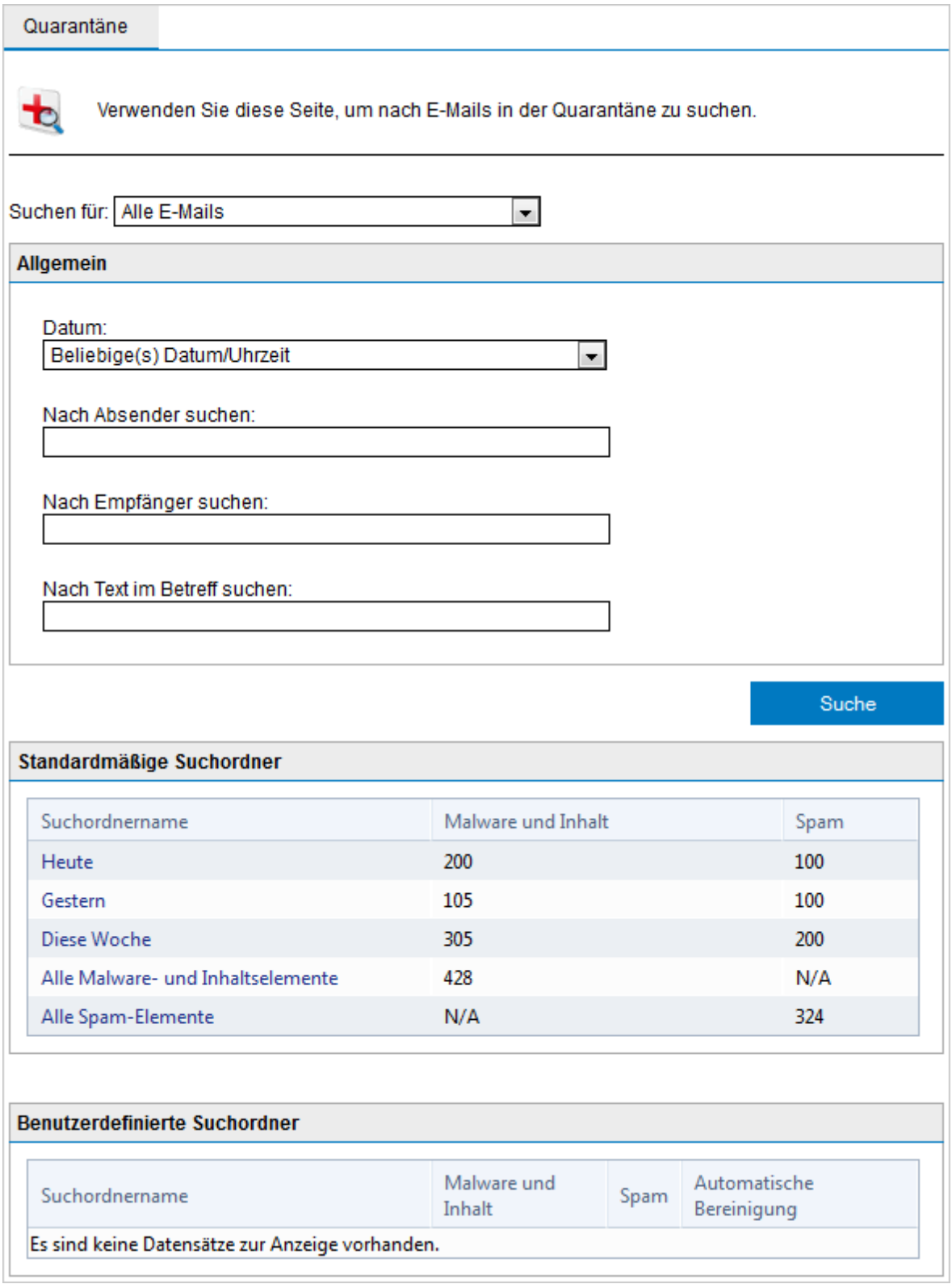
HINWEIS

Überprüfen Sie die E-Mails in Quarantäne anhand der Suchergebnisse. Falsch-positive Ergebnisse können zur Zustellung an die Empfänger bestätigt werden. Weitere Informationen finden Sie unter „Arbeiten mit E-Mails in Quarantäne“ (Seite 217).

8.3.1 Standardmäßige Suchordner

Standardmäßige Suchordner sind vorkonfigurierte Suchordner, die den Zugriff auf E-Mails in der Quarantäne anhand bestimmter Zeiträume oder eines bestimmten E-Mail-Typs ermöglichen. So verwenden Sie die standardmäßigen Suchordner:

1. Wählen Sie den Knoten **Quarantäne** aus.



Screenshot 112: Standardmäßige Suchordner

2. Wählen Sie im Bereich **Standardmäßige Suchordner** oder in einem Knoten unter dem Knoten **Quarantäne** einen Suchordner aus. GFI MailEssentials sucht automatisch nach allen E-Mails in der Quarantäne, die den Suchkriterien dieses Standardordners entsprechen, und zeigt sie an.

Folgende standardmäßige Suchordner sind verfügbar:

- **Zeitbasiert:**
  - Heute
  - Gestern
  - Diese Woche
- **Kategoriebasiert:**
  - Alle Malware- und Inhaltsfilter-Elemente
  - Alle Spam-Elemente

> **HINWEIS**
>
> Überprüfen Sie die E-Mails in Quarantäne anhand der Suchergebnisse. Falsch-positive Ergebnisse können zur Zustellung an die Empfänger bestätigt werden. Weitere Informationen finden Sie unter „Arbeiten mit E-Mails in Quarantäne“ (Seite 217).

8.3.2 Erstellen, Bearbeiten und Entfernen von benutzerdefinierten Suchordnern

1. Wählen Sie den Knoten **Quarantäne** aus.

2. Erstellen Sie eine neue Suche für E-Mails in der Quarantäne. Weitere Informationen finden Sie unter „Durchsuchen der Quarantäne“ (Seite 208).

3. Klicken Sie auf der Ergebnisseite auf **Als Suchordner speichern**, und geben Sie einen aussagekräftigen Namen für den neuen Suchordner ein.

Der neu erstellte Suchordner wird im Knoten **Quarantäne > Suchordner** aufgelistet.

> **HINWEIS**
>
> Wählen Sie zum Bearbeiten oder Löschen eines zuvor erstellten Suchordners diesen aus, und klicken Sie auf **Suchordner bearbeiten** oder **Suchordner löschen**.

8.3.3 Suchordnerknoten für die automatische Bereinigung von E-Mails in Quarantäne verwenden

Über den Knoten **Suchordner** können Sie Suchordnern erstellen und einen Wert für die automatische Bereinigung (in Tagen) festlegen. Überschreitet eine E-Mail in der Quarantäne die angegebene Anzahl an Tagen, wird sie gelöscht.

1. Wählen Sie den Knoten **Quarantäne > Suchordner** aus.

2. Konfigurieren Sie mithilfe der Anleitung in diesem Kapitel einen neuen Suchordner für E-Mails, die regelmäßig bereinigt werden sollen.

3. Wählen Sie **Automatische Bereinigung aktivieren** aus, und geben Sie an, für wie viele Tage die E-Mails aufbewahrt werden sollen.

4. Klicken Sie auf **Ordner speichern**.

8.4 Arbeiten mit E-Mails in Quarantäne

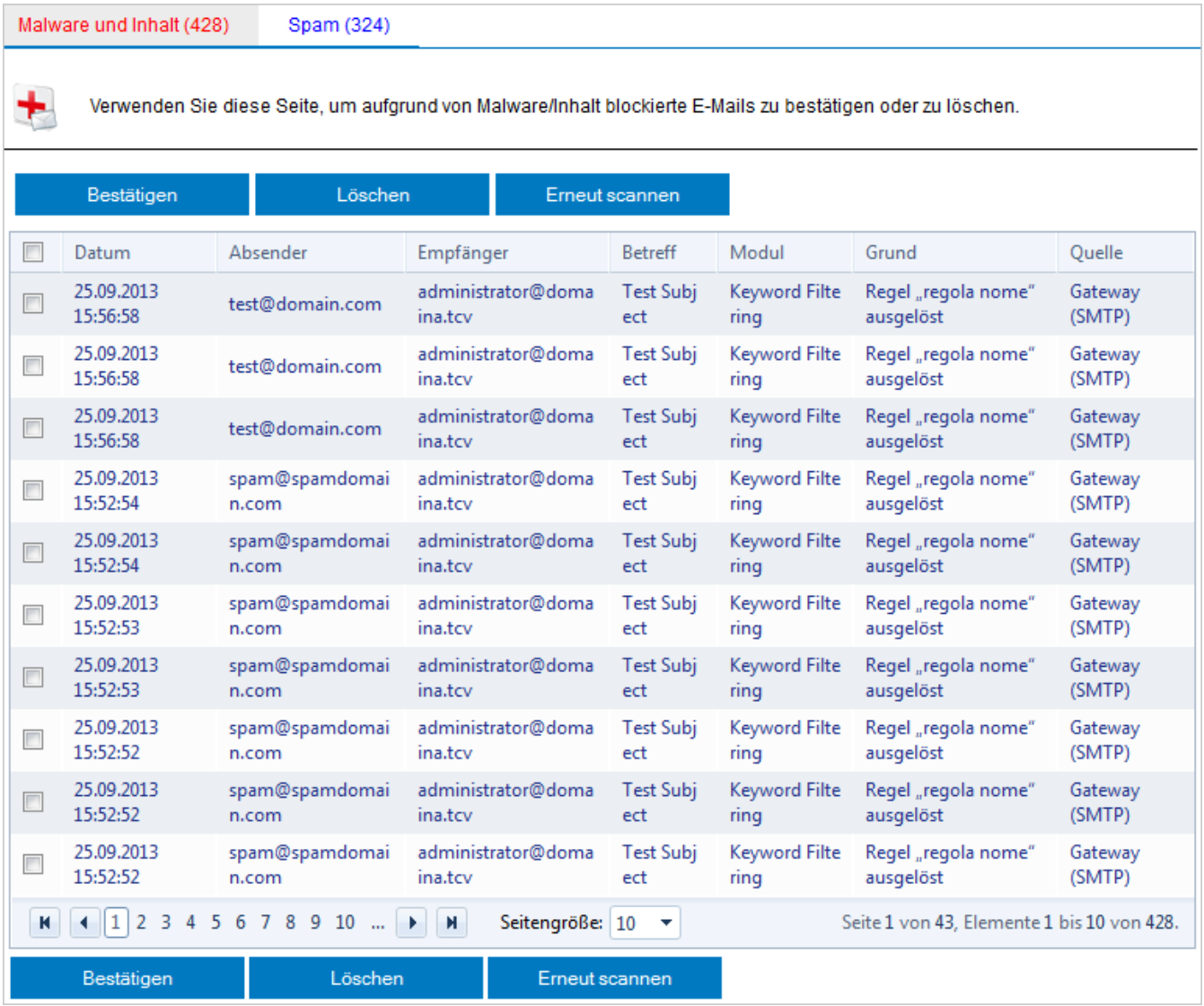
Sie können in GFI MailEssentials verschiedene Aktionen für E-Mails in der Quarantäne ausführen.

Der Quarantänespeicher ist über die GFI MailEssentials-Oberfläche zugänglich und ermöglicht dem Administrator die Verwaltung von E-Mails in der Quarantäne.

Zum Öffnen des Quarantänespeichers von GFI MailEssentials wählen Sie **GFI MailEssentials > Quarantäne** aus.

8.4.1 Anzeigen von E-Mails in der Quarantäne

Sie können die Quarantäne durchsuchen oder standardmäßige und benutzerdefinierte Suchordner verwenden, um eine Liste von E-Mails in der Quarantäne anzuzeigen.



Screenshot 113: Suchergebnisse

HINWEIS

Auf der Ergebnisseite können zwei Registerkarten angezeigt werden:

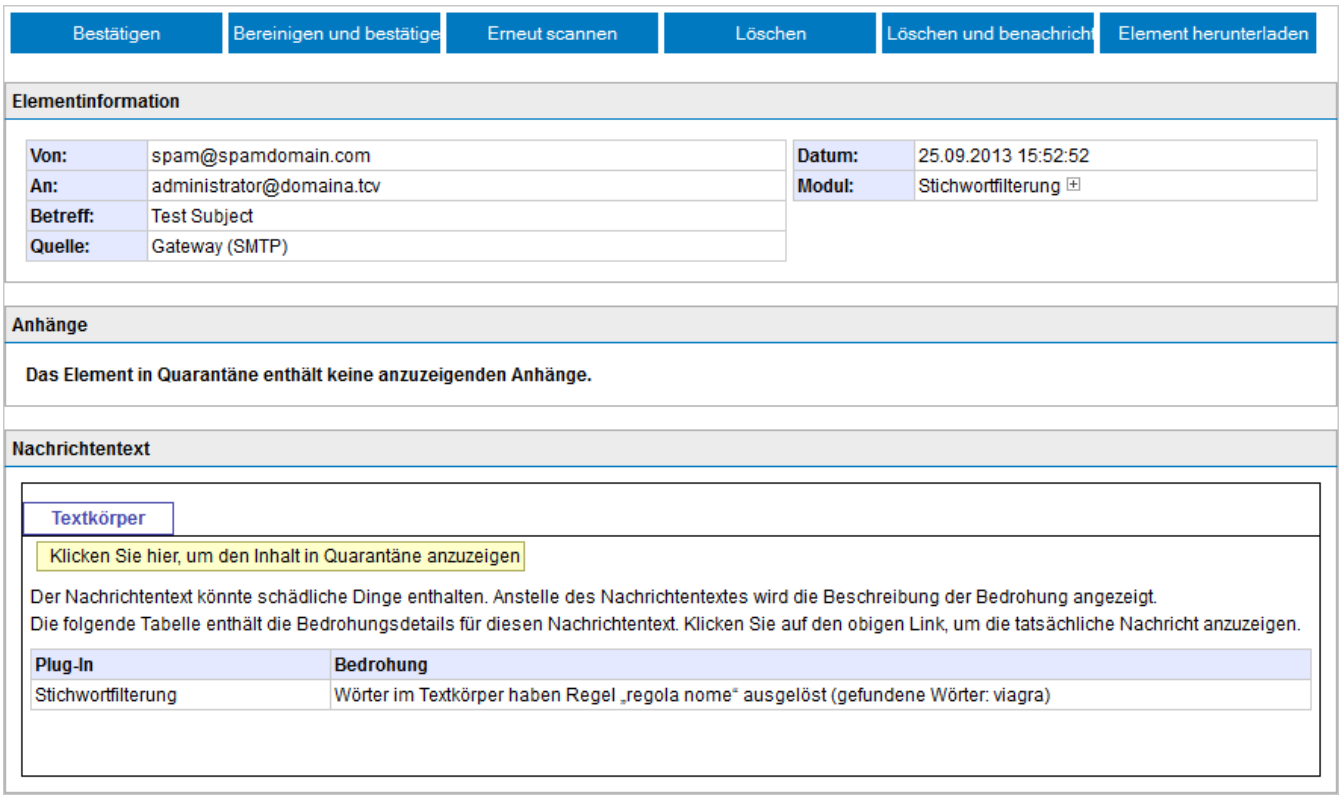
» **Malware und Inhalt** – E-Mails, die durch Malware-Engines und Inhaltsfilterungsregeln blockiert wurden.

» **Spam** – E-Mails, die durch Anti-Spam-Filter blockiert wurden.

1. Wählen Sie die Registerkarte **Malware und Inhalt** oder **Spam** aus, um die entsprechenden E-Mails in der Quarantäne anzuzeigen. Die Ergebnisseite bietet folgende Funktionen und Informationen:

Option	Beschreibung
Zurück	Sie kehren zum vorherigen Bildschirm zurück.
Bestätigen	Sie können eine oder mehrere E-Mails bestätigen. Weitere Informationen finden Sie unter „Bestätigen von E-Mails in Quarantäne “ (Seite 220).
Löschen	Löscht eine oder mehrere E-Mails. Weitere Informationen finden Sie unter „Dauerhaftes Löschen von E-Mails in Quarantäne “ (Seite 220).
Erneut scannen	Scannt E-Mails erneut mit den aktuellen Anti-Virus-Signaturen (die vermutlich aktueller sind als zu dem Zeitpunkt, zu dem die E-Mails in die Quarantäne verschoben wurden). Wählen Sie eine oder mehrere E-Mails aus, und klicken Sie auf **Erneut scannen**.
Modul	Das Modul, mit dem die E-Mail in die Quarantäne verschoben wurde
Grund	Die Ursache/Regel, die das Verschieben der E-Mail in die Quarantäne ausgelöst hat
Absender	Die E-Mail-Adresse des Absenders
Empfänger	Die E-Mail-Adresse des Empfängers
Betreff	Der E-Mail-Betreff, wie vom Absender angegeben
Datum	Das Datum, an dem die E-Mail in die Quarantäne verschoben wurde
Quelle	Der Ort, von dem die E-Mail in die Quarantäne verschoben wurde
Elementquelle	Ermöglicht die Auswahl einer Quelle, nach der die Anzeige gefiltert wird. Folgende Optionen sind verfügbar: » Alle anzeigen » Informationsspeicher (VSAPI) » Gateway (SMTP) » Informationsspeicher (Transport)
Seitengröße	Sie können festlegen, wie viele E-Mails pro Seite angezeigt werden sollen. Wählen Sie die maximale Anzahl an Elementen pro Seite aus.

2. Klicken Sie auf eine Zeile, um Informationen zur jeweiligen E-Mail anzuzeigen.


Bestätigen
Bereinigen und bestätige
Erneut scannen
Löschen
Löschen und benachricht
Element herunterladen
Elementinformation
Von: spam@spamdomain.com
An: administrator@domaina.tcv
Betreff: Test Subject
Quelle: Gateway (SMTP)
Datum: 25.09.2013 15:52:52
Modul: Stichwortfilterung
Anhänge
Das Element in Quarantäne enthält keine anzuzeigenden Anhänge.
Nachrichtentext
Textkörper
Klicken Sie hier, um den Inhalt in Quarantäne anzuzeigen
Der Nachrichtentext könnte schädliche Dinge enthalten. Anstelle des Nachrichtentextes wird die Beschreibung der Bedrohung angezeigt.
Die folgende Tabelle enthält die Bedrohungsdetails für diesen Nachrichtentext. Klicken Sie auf den obigen Link, um die tatsächliche Nachricht anzuzeigen.
Plug-In
Bedrohung
Stichwortfilterung
Wörter im Textkörper haben Regel „regola nome“ ausgelöst (gefundene Wörter: viagra)

Screenshot 114: Details zu Elementen in Quarantäne

Auf der Seite mit **Details zu Elementen in Quarantäne** können Sie Informationen zur jeweiligen E-Mail anzeigen und folgende Aktionen ausführen.

Aktion	Beschreibung
Bestätigen	Bestätigt die E-Mail. Weitere Informationen finden Sie unter „Bestätigen von E-Mails in Quarantäne “ (Seite 220).
Bereinigen und bestätigen	Bereinigt und bestätigt die E-Mail. Weitere Informationen finden Sie unter „Bestätigen von E-Mails in Quarantäne “ (Seite 220).
Erneut scannen	Scannt E-Mails erneut mit den aktuellen Anti-Virus-Signaturen (die vermutlich aktueller sind als zu dem Zeitpunkt, zu dem die E-Mails in die Quarantäne verschoben wurden).
Löschen	Löscht die E-Mail. Weitere Informationen finden Sie unter „Dauerhaftes Löschen von E-Mails in Quarantäne “ (Seite 220).
Löschen und benachrichtigen	Löscht die E-Mail und benachrichtigt den Benutzer. Weitere Informationen finden Sie unter „Dauerhaftes Löschen von E-Mails in Quarantäne “ (Seite 220).
Element herunterladen	Lädt die E-Mail aus der Quarantäne im EML-Format an einen von Ihnen gewählten Speicherort herunter. **Warnhinweis:** **E-Mails im Quarantänespeicher können schädliche Inhalte aufweisen. Diese Funktion ist mit Vorsicht zu verwenden.**

8.4.2 Bestätigen von E-Mails in Quarantäne

Es kann vorkommen, dass Sie eine E-Mail zulassen möchten, die von GFI MailEssentials blockiert wurde. GFI MailEssentials bietet Administratoren die Möglichkeit, E-Mails in der Quarantäne zu bestätigen, so dass sie aus dem Quarantänespeicher entfernt und an den jeweiligen Empfänger zugestellt werden.

So bestätigen Sie E-Mails:

1. Verwenden Sie die in den vorherigen Abschnitten beschriebenen Suchfunktionen, um eine Liste von E-Mails in der Quarantäne anzuzeigen.

2. Aktivieren Sie die Kontrollkästchen der Quarantäne-E-Mails, die bestätigt werden sollen, und klicken Sie auf **Bestätigen**.

Bereinigen und Bestätigen von E-Mails

GFI MailEssentials bietet auch die Möglichkeit, das Element zu entfernen, aufgrund dessen eine E-Mail in die Quarantäne verschoben wurde, und die E-Mail dann an den Empfänger zu senden.

So bereinigen und bestätigen Sie E-Mails:

1. Verwenden Sie die in den vorherigen Abschnitten beschriebenen Suchfunktionen, um eine Liste von E-Mails in der Quarantäne anzuzeigen.

2. Klicken Sie auf eine E-Mail, um ihre Details anzuzeigen.

3. Klicken Sie auf **Bereinigen und bestätigen**.

> **HINWEIS**
>
> E-Mails, die aus dem Informationsspeicher (VSAPI) in die Quarantäne verschoben wurden, können nicht bereinigt werden.

8.4.3 Dauerhaftes Löschen von E-Mails in Quarantäne

1. Verwenden Sie die in den vorherigen Abschnitten beschriebenen Suchfunktionen, um eine Liste von

E-Mails in der Quarantäne anzuzeigen.

2. Aktivieren Sie die Kontrollkästchen der gewünschten Quarantäne-E-Mails, und klicken Sie auf **Löschen**.

E-Mails in Quarantäne löschen und Benutzer benachrichtigen

Mit der Funktion zum Löschen und Benachrichtigen können Sie die Empfänger benachrichtigen, wenn E-Mails in der Quarantäne gelöscht werden.

So können Sie E-Mails löschen und die Empfänger benachrichtigen:

1. Verwenden Sie die in den vorherigen Abschnitten beschriebenen Suchfunktionen, um eine Liste von E-Mails in der Quarantäne anzuzeigen.

2. Klicken Sie auf eine E-Mail, um ihre Details anzuzeigen.

3. Klicken Sie auf **Löschen und benachrichtigen**.

8.5 Quarantäne-RSS-Feeds

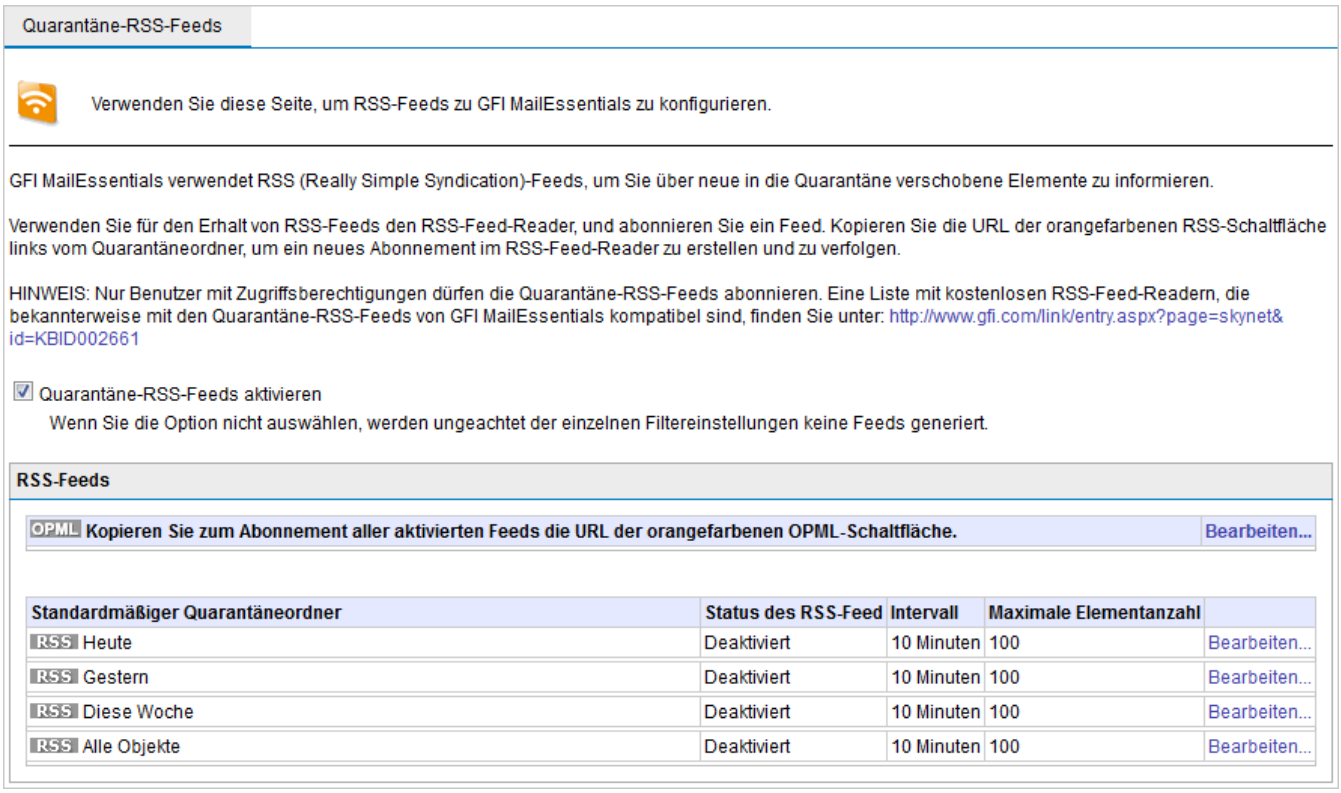
RSS (Really Simple Syndication) ist ein Protokoll, das zur Verteilung von häufig aktualisierten Inhalten oder Feeds (z. B. Nachrichten) an die Abonnenten verwendet wird. Zum Anzeigen der RSS-Feeds benötigen die Abonnenten einen RSS-Feed-Reader. RSS-Feeds beinhalten üblicherweise eine Zusammenfassung des Inhalts und einen Link zum vollständigen Artikel.

RSS-Feeds können auch zur Überwachung von E-Mails in der Quarantäne verwendet werden. Die Quarantäne-RSS-Feeds von GFI MailEssentials zeigen die E-Mails in der Quarantäne, die überprüft werden müssen, und bieten den Benutzern die Möglichkeit, E-Mails in der Quarantäne zu bestätigen oder zu löschen.

> **HINWEIS**
>
> Die Quarantäne-RSS-Feeds von GFI MailEssentials können mit den meisten RSS-Feed-Readern verwendet werden. Eine Liste von kostenlosen RSS-Feed-Readern, die mit den Quarantäne-RSS-Feeds von GFI MailEssentials getestet wurden, finden Sie unter:
>
> http://kbase.gfi.com/showarticle.asp?id=KBID002661

8.5.1 Aktivieren von Quarantäne-RSS-Feeds

1. Wählen Sie **GFI MailEssentials > Quarantäne > Quarantäne-RSS-Feeds** aus.


Quarantäne-RSS-Feeds
Verwenden Sie diese Seite, um RSS-Feeds zu GFI MailEssentials zu konfigurieren.
GFI MailEssentials verwendet RSS (Really Simple Syndication)-Feeds, um Sie über neue in die Quarantäne verschobene Elemente zu informieren.
Verwenden Sie für den Erhalt von RSS-Feeds den RSS-Feed-Reader, und abonnieren Sie ein Feed. Kopieren Sie die URL der orangefarbenen RSS-Schaltfläche links vom Quarantäneordner, um ein neues Abonnement im RSS-Feed-Reader zu erstellen und zu verfolgen.
HINWEIS: Nur Benutzer mit Zugriffsberechtigungen dürfen die Quarantäne-RSS-Feeds abonnieren. Eine Liste mit kostenlosen RSS-Feed-Readern, die bekannterweise mit den Quarantäne-RSS-Feeds von GFI MailEssentials kompatibel sind, finden Sie unter: http://www.gfi.com/link/entry.aspx?page=skynet&id=KBID002661
Quarantäne-RSS-Feeds aktivieren
Wenn Sie die Option nicht auswählen, werden ungeachtet der einzelnen Filtereinstellungen keine Feeds generiert.
RSS-Feeds
OPML Kopieren Sie zum Abonnement aller aktivierten Feeds die URL der orangefarbenen OPML-Schaltfläche.
Bearbeiten...
Standardmäßiger Quarantäneordner
Status des RSS-Feed
Intervall
Maximale Elementanzahl
RSS Heute
Deaktiviert
10 Minuten
100
Bearbeiten...
RSS Gestern
Deaktiviert
10 Minuten
100
Bearbeiten...
RSS Diese Woche
Deaktiviert
10 Minuten
100
Bearbeiten...
RSS Alle Objekte
Deaktiviert
10 Minuten
100
Bearbeiten...

Screenshot 115: Quarantäne-RSS-Feeds

2. Markieren Sie das Kontrollkästchen **Quarantäne-RSS-Feeds aktivieren**.

3. Klicken Sie im Bereich **RSS-Feeds** rechts neben dem Quarantänesuchordner, für den Sie RSS-Feeds aktivieren möchten, auf **Bearbeiten**.

4. Markieren Sie das Kontrollkästchen **Quarantäne-RSS-Feeds für diesen Ordner aktivieren**.

5. Geben Sie im Textfeld **Feed-Inhalt aktualisieren alle** das Aktualisierungsintervall in Minuten an. Der Standardwert beträgt 10 Minuten.

6. Geben Sie die maximale Anzahl an Elementen, die ein Feed enthalten darf, im Textfeld **Feed darf höchstens enthalten** an. Der Standardwert beträgt 100 Elemente.

> **HINWEIS**
>
> Sie können die URL eines RSS-Feeds ändern, indem Sie auf **Feed-URL zurücksetzen** klicken. Um die URL für alle aktivierten RSS-Feeds zu ändern, klicken Sie neben dem **OPML**-Eintrag auf **Bearbeiten**, und klicken Sie dann auf **Alle URLs zurücksetzen**. Wenn Sie URLs ändern, stellen Sie sicher, dass Sie auch alle vorhandenen Abonnements entsprechend aktualisieren.
>
> Das Zurücksetzen einer Feed-URL sollte im Falle eines unberechtigten Zugriffs erfolgen.

7. Klicken Sie auf **Übernehmen**.

8.5.2 Abonnieren von Quarantäne-RSS-Feeds

Abonnieren von allen aktivierten Quarantäne-RSS-Feeds

1. Wählen Sie **GFI MailEssentials > Quarantäne > Quarantäne-RSS-Feeds** aus.

2. Klicken Sie im RSS-Feeds-Bereich mit der rechten Maustaste auf das Symbol OPML, und klicken Sie auf **Verknüpfung kopieren**, um die URL des RSS-Feeds zu kopieren.

3. Erstellen Sie mit der kopierten URL in Ihrem RSS-Feed-Reader ein neues RSS-Feed-Abonnement.

Abonnieren eines Quarantäne-RSS-Feeds eines Suchordners

So abonnieren Sie ein RSS-Feed eines standardmäßigen oder benutzerdefinierten Suchordners:

1. Wählen Sie **GFI MailEssentials > Quarantäne > Quarantäne-RSS-Feeds** aus.

2. Klicken Sie im RSS-Feeds-Bereich mit der rechten Maustaste auf das Symbol RSS neben dem gewünschten Suchordner, und klicken Sie auf **Verknüpfung kopieren**, um die URL des RSS-Feeds zu kopieren.

3. Erstellen Sie mit der kopierten URL in Ihrem RSS-Feed-Reader ein neues RSS-Feed-Abonnement.

8.5.3 Sichern des Zugriffs auf die Quarantäne-RSS-Feeds von GFI MailEssentials

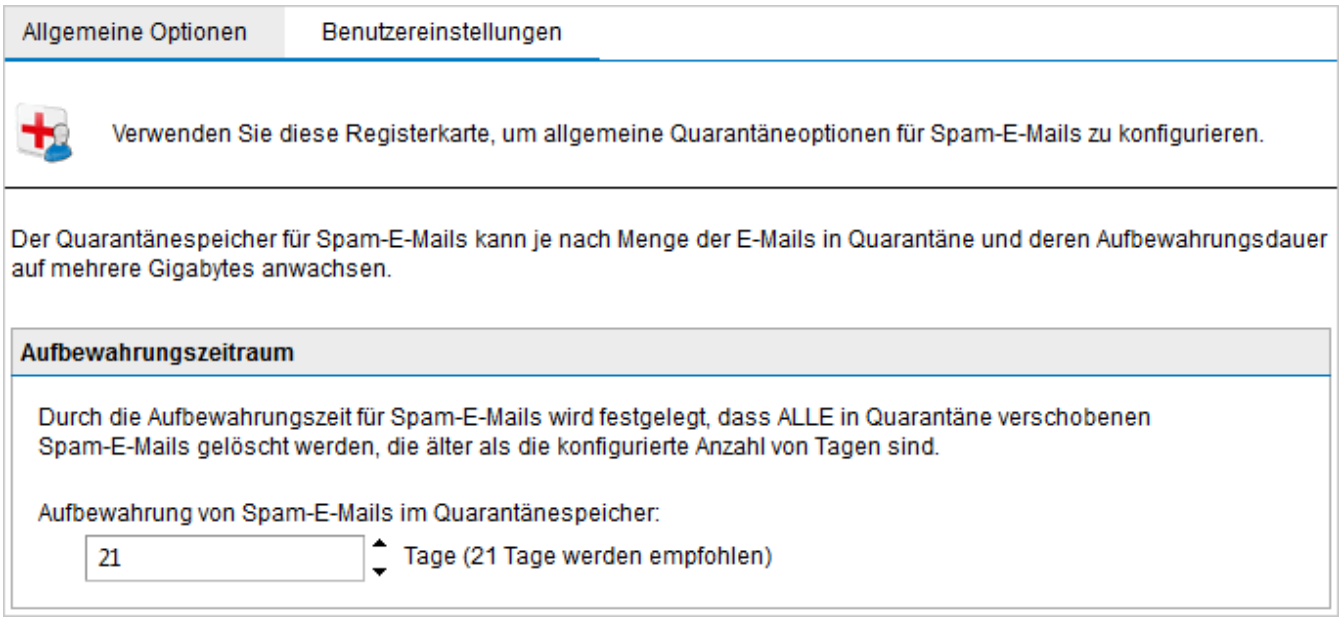
In GFI MailEssentials Configuration können Sie im Knoten für die Zugriffssteuerung festlegen, wer die Quarantäne-RSS-Feeds abonnieren darf. Weitere Informationen finden Sie unter „Zugriffssteuerung“ (Seite 251).

8.6 Quarantäneoptionen

Konfigurieren Sie mithilfe der Quarantäneoptionen die Aufbewahrungsdauer für Spam in der Quarantäne, die Benutzerberichterstellung und den Umgang mit Malware-Nachrichten, die an nicht vorhandene Benutzer adressiert sind.

8.6.1 Spam-Optionen

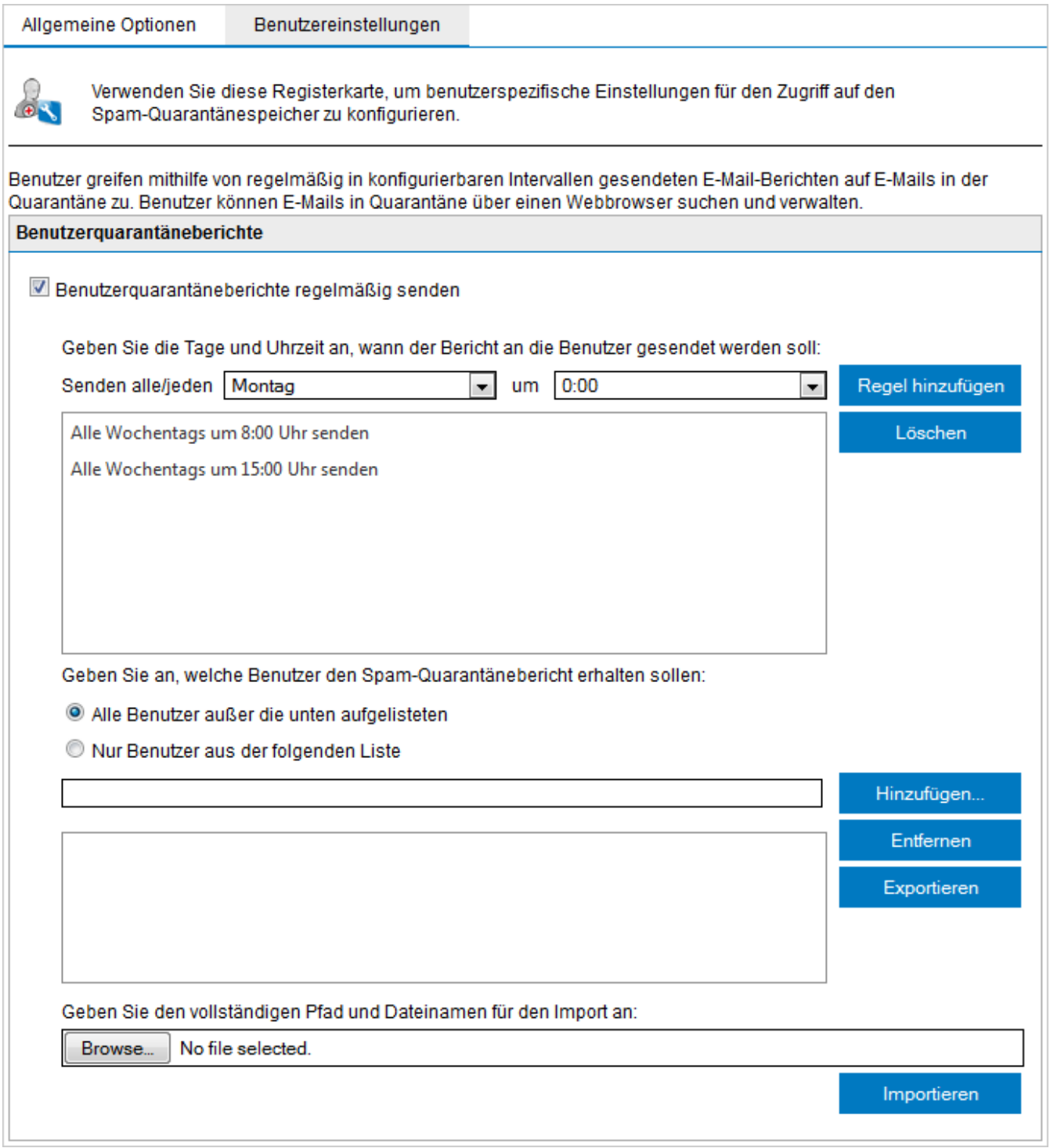
1. Wählen Sie **Quarantäne > Quarantäneoptionen > Spam-Optionen** aus.


Allgemeine Optionen
Benutzereinstellungen
Verwenden Sie diese Registerkarte, um allgemeine Quarantäneoptionen für Spam-E-Mails zu konfigurieren.
Der Quarantänespeicher für Spam-E-Mails kann je nach Menge der E-Mails in Quarantäne und deren Aufbewahrungsdauer auf mehrere Gigabytes anwachsen.
Aufbewahrungszeitraum
Durch die Aufbewahrungszeit für Spam-E-Mails wird festgelegt, dass ALLE in Quarantäne verschobenen Spam-E-Mails gelöscht werden, die älter als die konfigurierte Anzahl von Tagen sind.
Aufbewahrung von Spam-E-Mails im Quarantänespeicher:
21
Tage (21 Tage werden empfohlen)

Screenshot 116: Spam-Optionen - Registerkarte für allgemeine Optionen

2. Legen Sie auf der Registerkarte **Allgemeine Optionen** die Zeitdauer der **Aufbewahrung von Spam-E-Mails im Quarantänespeicher** fest.

3. Klicken Sie auf die Registerkarte **Benutzereinstellungen**.


Allgemeine Optionen
Benutzereinstellungen
Verwenden Sie diese Registerkarte, um benutzerspezifische Einstellungen für den Zugriff auf den Spam-Quarantänespeicher zu konfigurieren.
Benutzer greifen mithilfe von regelmäßig in konfigurierbaren Intervallen gesendeten E-Mail-Berichten auf E-Mails in der Quarantäne zu. Benutzer können E-Mails in Quarantäne über einen Webbrowser suchen und verwalten.
Benutzerquarantäneberichte
Benutzerquarantäneberichte regelmäßig senden
Geben Sie die Tage und Uhrzeit an, wann der Bericht an die Benutzer gesendet werden soll:
Senden alle/jeden
Montag
um
0:00
Regel hinzufügen
Löschen
Alle Wochentags um 8:00 Uhr senden
Alle Wochentags um 15:00 Uhr senden
Geben Sie an, welche Benutzer den Spam-Quarantänebericht erhalten sollen:
Alle Benutzer außer die unten aufgelisteten
Nur Benutzer aus der folgenden Liste
Hinzufügen...
Entfernen
Exportieren
Geben Sie den vollständigen Pfad und Dateinamen für den Import an:
Browse...
No file selected.
Importieren

Screenshot 117: Spam-Optionen - Registerkarte für Benutzereinstellungen

4. Wählen Sie **Benutzerquarantäneberichte regelmäßig senden** aus, um das Senden von Benutzerquarantäneberichten zu aktivieren.

HINWEIS

Benutzerquarantäneberichte sind regelmäßige E-Mails an die E-Mail-Benutzer, die eine Liste der blockierten E-Mails für den betreffenden Benutzer enthalten. Die Benutzer können die Liste überprüfen, um zulässige E-Mails, die blockiert wurden, zuzulassen. E-Mails, die von der Malware- und Inhaltsfilterung blockiert wurden, werden hier nicht angezeigt.

5. Legen Sie fest, wie oft Berichte gesendet werden sollen. Sie können den vordefinierten Zeitplan ergänzen, indem Sie ein Datum und eine Uhrzeit auswählen und auf **Regel hinzufügen** klicken. Wählen Sie zum Löschen eines vorhandenen Eintrags (Datum und Uhrzeit) diesen aus, und klicken Sie auf **Löschen**.

6. Konfigurieren Sie die Benutzer, die Berichte über Spam in der Quarantäne erhalten sollen. Wählen Sie **Alle Benutzer außer die unten aufgelisteten** oder **Nur Benutzer aus der folgenden Liste** aus, und geben Sie die E-Mail-Adressen der Benutzer an, die ein- oder ausgeschlossen werden sollen.

> **HINWEIS**
>
> Klicken Sie auf **Durchsuchen**, um eine Datei mit einer Liste von E-Mail-Adressen auszuwählen und diese zu **Importieren**.

7. Klicken Sie auf **Übernehmen**.

8.6.2 Malware-Optionen

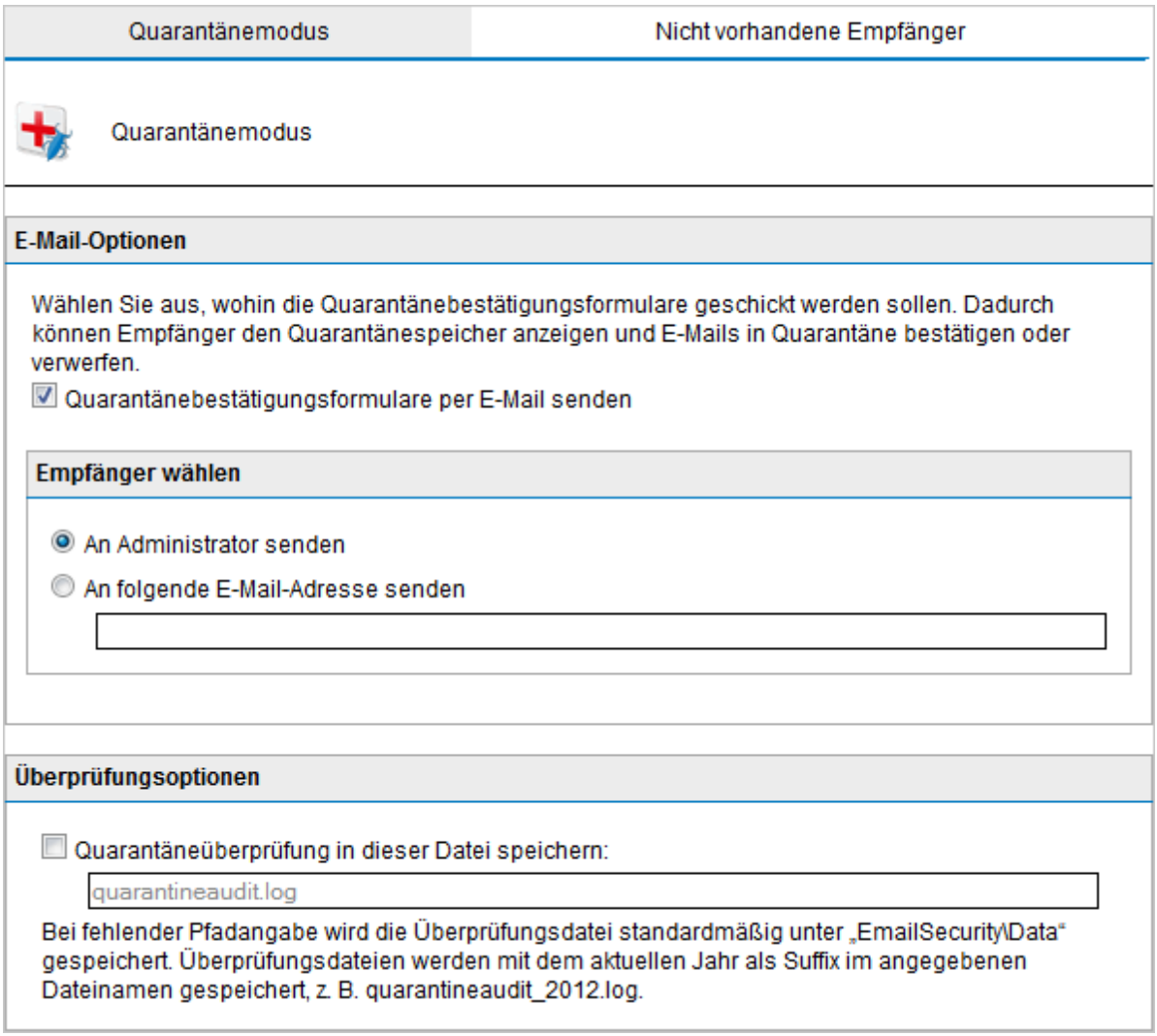
GFI MailEssentials kann auch den Administrator oder andere berechtigte Benutzer per E-Mail benachrichtigen (Formular für Quarantäneaktion), wenn eine E-Mail in die Quarantäne verschoben wird.

Das Quarantänebestätigungsformulare enthält Details zu der unter Quarantäne gestellten E-Mail, z. B. die Begründung für die Blockierung und ggf. die Anhänge der E-Mail. Der Administrator kann die unter Quarantäne gestellte E-Mail dann direkt im E-Mail-Client bearbeiten (z. B. zulassen).

> **HINWEIS**
>
> Wenn Sie E-Mails, die älter als eine bestimmte Anzahl von Tagen sind, automatisch löschen möchten, erstellen Sie einen neuen Suchordner, und stellen Sie die automatische Bereinigungsfunktion so ein, dass E-Mails nach der gewünschten Anzahl von Tagen gelöscht werden. Weitere Informationen finden Sie unter „Suchordnerknoten für die automatische Bereinigung von E-Mails in Quarantäne verwenden “ (Seite 217).

Aktivieren von Quarantänebestätigungsformularen

1. Wählen Sie **Quarantäne > Quarantäneoptionen > Malware-Optionen** aus.


Quarantänemodus
Nicht vorhandene Empfänger
Quarantänemodus
E-Mail-Optionen
Wählen Sie aus, wohin die Quarantänebestätigungsformulare geschickt werden sollen. Dadurch können Empfänger den Quarantänespeicher anzeigen und E-Mails in Quarantäne bestätigen oder verwerfen.
Quarantänebestätigungsformulare per E-Mail senden
Empfänger wählen
An Administrator senden
An folgende E-Mail-Adresse senden
Überprüfungsoptionen
Quarantäneüberprüfung in dieser Datei speichern:
quarantineaudit.log
Bei fehlender Pfadangabe wird die Überprüfungsdatei standardmäßig unter „EmailSecurity\Data" gespeichert. Überprüfungsdateien werden mit dem aktuellen Jahr als Suffix im angegebenen Dateinamen gespeichert, z. B. quarantineaudit_2012.log.

Screenshot 118: Quarantänemodus

2. Wählen Sie auf der Registerkarte **Quarantänemodus** das Kontrollkästchen **Quarantänebestätigungsformulare per E-Mail senden**, um das Senden von Quarantänebestätigungsformularen zu aktivieren.

3. Geben Sie im Bereich **Empfänger wählen** den Empfänger der Quarantänebestätigungsformulare an:

Option	Beschreibung
An Administrator senden	Sendet Quarantänebestätigungsformulare an den Administrator, wie im Knoten **Allgemeine Einstellungen** konfiguriert. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse (Seite 245)“.
An folgende E-Mail-Adresse senden	Sendet Quarantänebestätigungsformulare an eine andere E-Mail-Adresse. Geben Sie den Empfänger im vorgesehenen Textfeld ein.

4. Optional: Wählen Sie **Quarantäneüberprüfung in dieser Datei speichern** aus, und konfigurieren Sie einen Dateinamen, unter dem eine Kopie des Quarantäneprotokolls gespeichert werden soll.

5. Klicken Sie auf **Übernehmen**.

Nicht vorhandene Empfänger

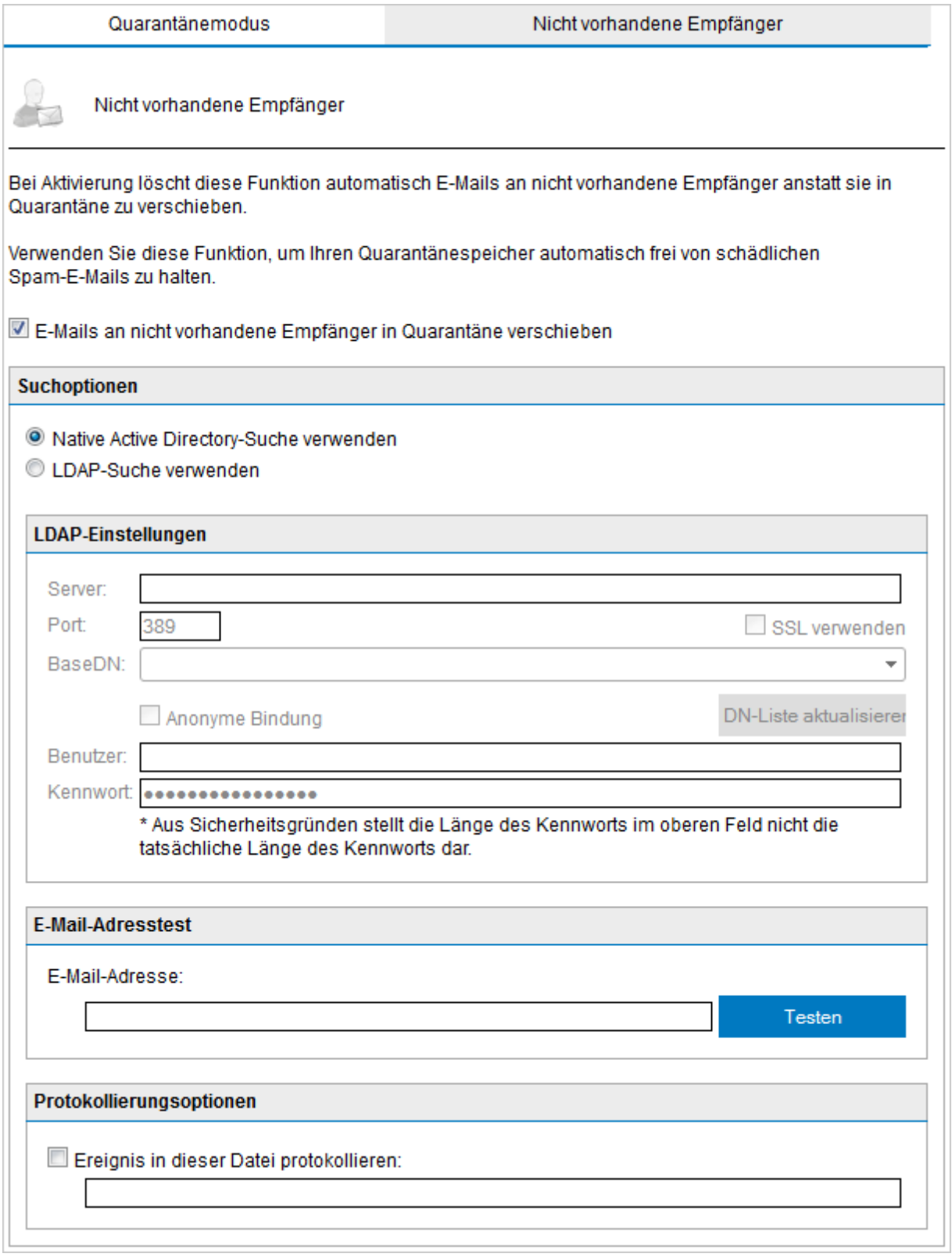
Die GFI MailEssentials-Funktion für nicht vorhandene Empfänger scannt E-Mails auf nicht vorhandene lokale E-Mail-Adressen, bevor sie in den Quarantänespeicher verschoben werden. Enthält eine E-Mail

eine nicht vorhandene lokale E-Mail-Adresse, wird sie dauerhaft gelöscht. Dies reduziert die Anzahl der E-Mails, die vom Administrator überprüft werden müssen.

Konfigurieren des Filters für nicht vorhandene Empfänger

Der Filter für nicht vorhandene Empfänger benötigt Zugriff auf die Liste der lokalen Adressen. Dieser erfolgt entweder über Active Directory oder – falls keine Kommunikation mit Active Directory möglich ist – über einen LDAP-Server.

1. Wählen Sie **Quarantäne > Quarantäneoptionen > Malware-Optionen** aus.



Screenshot 119: Nicht vorhandene Empfänger

2. Aktivieren Sie auf der Registerkarte **Nicht vorhandene Empfänger** das Kontrollkästchen**E-Mails an nicht vorhandene Empfänger in Quarantäne verschieben.**

3. Wählen Sie die Methode für die Suche nach Benutzern aus:

Option	Beschreibung
Native Active Directory-Suche verwenden	Wählen Sie diese Option aus, wenn GFI MailEssentials im Active Directory-Modus installiert ist und Zugriff auf ALLE Benutzer in Active Directory hat. Fahren Sie mit Schritt 8 fort. **HINWEIS** Ist GFI MailEssentials im Active Directory-Modus in einer DMZ installiert, sind im Active Directory der DMZ üblicherweise nicht alle Netzwerkbenutzer (E-Mail-Empfänger) verzeichnet. Konfigurieren Sie GFI MailEssentials in diesem Fall so, dass die LDAP-Suche verwendet wird. **HINWEIS** Wird GFI MailEssentials hinter einer Firewall betrieben, kann diese Funktion möglicherweise aufgrund der Firewall-Einstellungen keine direkte Verbindung mit dem internen Active Directory herstellen. Verwenden Sie für die Verbindung mit dem internen Active Directory Ihres Netzwerks die LDAP-Suche, und stellen Sie sicher, dass der Standardport 389 in Ihrer Firewall aktiviert ist.
LDAP-Suche verwenden	Wählen Sie diese Option aus, wenn GFI MailEssentials im SMTP-Modus installiert ist und/oder wenn GFI MailEssentials keinen direkten Zugriff auf die vollständige Liste der Benutzer hat.

4. Geben Sie den LDAP-Servernamen oder die IP-Adresse im Textfeld **Server** ein.

> **HINWEIS**
>
> In einer Active Directory-Umgebung ist der LDAP-Server üblicherweise der Domänencontroller oder der Global Catalog.

5. Geben Sie die Portnummer (standardmäßig 389) im Textfeld **Port** ein. Erfolgt die Verbindung mit dem LDAP-Server über SSL, wählen Sie **SSL verwenden** aus. Der Standardport ist dann 636.

> **HINWEIS**
>
> Stellen Sie sicher, dass der Port in der Firewall aktiviert ist.

6. Klicken Sie auf **DN-Liste aktualisieren**, um die Liste **BaseDN** zu füllen, und wählen Sie den BaseDN aus (die oberste Ebene der Active Directory-Hierarchie).

7. Falls Ihr LDAP-Server eine Authentifizierung verlangt, geben Sie den **Benutzernamen** und das **Kennwort** ein. Wenn keine Authentifizierung erforderlich ist, wählen Sie **Anonyme Bindung** aus.

8. Testen Sie Ihre Konfigurationseinstellungen, indem Sie im Feld **E-Mail-Adresse** eine gültige E-Mail-Adresse eingeben und auf **Test** klicken. Wird die E-Mail-Adresse nicht gefunden, überprüfen Sie die Konfigurationseinstellungen.

9. Um die Aktivitäten des Filters für nicht vorhandene Empfänger zu protokollieren, wählen Sie **Ereignis in dieser Datei protokollieren** aus, und geben Sie den Pfad und Dateinamen (einschließlich TXT-Erweiterung) eines benutzerdefinierten Speicherorts auf der Festplatte an. Wenn Sie nur den Dateinamen angeben (einschließlich TXT-Erweiterung), wird die Protokolldatei im folgenden Standardverzeichnis gespeichert:

```
<GFI MailEssentials Installationspfad>\GFI\MailEssentials\\EmailSecurity\Logs\<Dateiname>.txt
```

10. Klicken Sie auf **Übernehmen**.

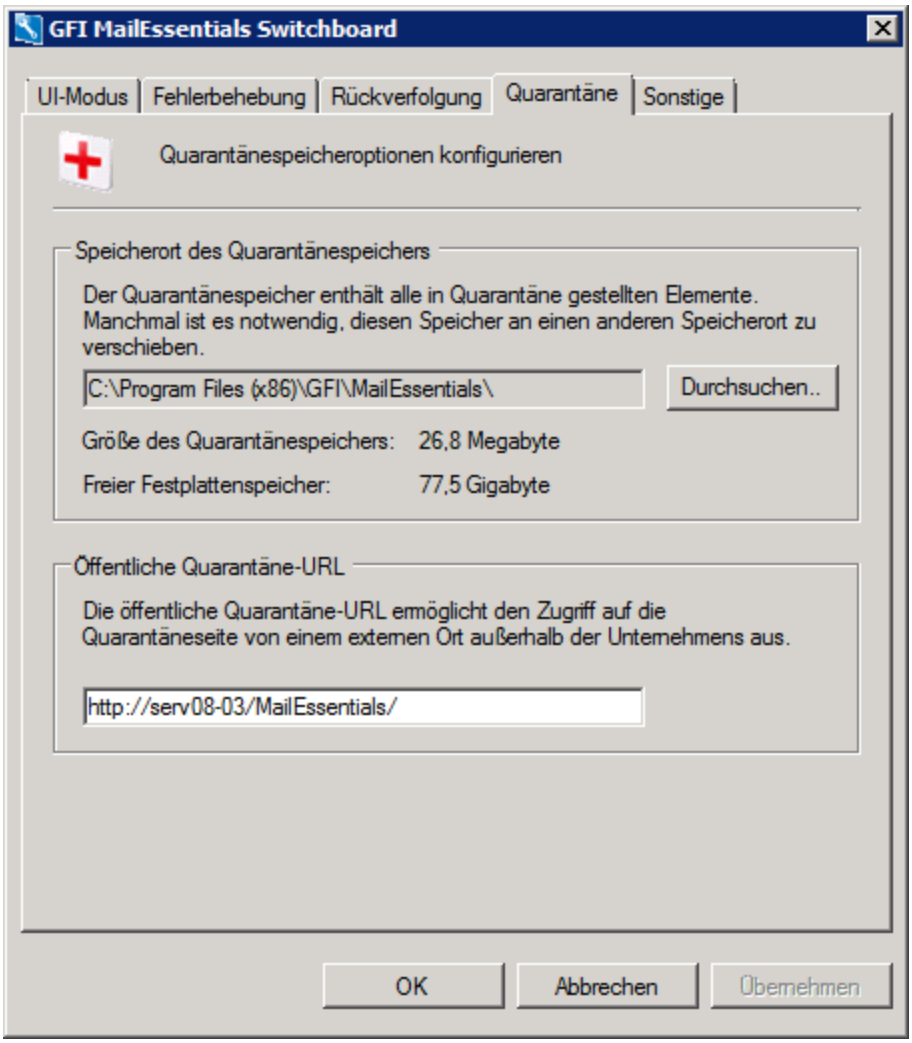
8.7 Speicherort des Quarantänespeichers und öffentliche URL

Verwenden Sie das GFI MailEssentials Switchboard, um den Speicherort des Quarantänespeichers und die öffentliche URL der Quarantäne festzulegen.

Am Speicherort des Quarantänespeichers werden E-Mails gespeichert, die unter Quarantäne gestellt wurden. Dieser befindet sich standardmäßig unter dem Installationspfad von GFI MailEssentials. In manchen Fällen kann es jedoch nötig sein, einen anderen Speicherort auszuwählen, z. B. wenn zu wenig Festplattenspeicher vorhanden ist.

Die öffentliche Quarantäne-URL ermöglicht den Zugriff auf die Quarantäneseite von einem externen Ort aus. Standardmäßig sind dafür die Einstellungen für das virtuelle IIS-Verzeichnis von GFI MailEssentials ausschlaggebend, die Sie bei der Installation festgelegt haben. Es kann jedoch nötig sein, dies zu ändern, wenn Sie Quarantäneübersicht-E-Mails oder Benachrichtigungen versenden möchten, die außerhalb des internen Netzwerks verfügbar sein sollen. Ändern Sie in diesem Fall die URL so, dass sie über das Internet zugänglich ist.

1. Starten Sie das GFI MailEssentials Switchboard über **Start > Programme > GFI MailEssentials > Switchboard**.



Screenshot 120: Speicherort des Quarantänespeichers und öffentliche URL

2. Klicken Sie auf der Registerkarte **Quarantäne** auf **Durchsuchen**, um einen anderen Speicherort für den Quarantänespeicher auszuwählen.

WICHTIG

Stellen Sie sicher, dass die Partition, auf der der Quarantänespeicher gespeichert werden soll, über ausreichend freien Speicherplatz verfügt. Spam-E-Mails werden nicht in die Quarantäne verschoben, wenn der freie Festplattenspeicher gleich oder kleiner als 512 MB ist. Beim Erreichen von 512 MB stellt die E-Mail-Quarantäne den Betrieb ein, Spam-E-Mails werden als solche gekennzeichnet und dem Empfängerpostfach zugestellt, bis der freie Speicherplatz größer als 512 MB ist.

3. Geben Sie eine URL an, mit der die Quarantäne von einem externen Ort außerhalb Ihres Unternehmens zugänglich ist.

4. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

9 E-Mail-Verwaltung

GFI MailEssentials beinhaltet eine Reihe von Tools für die Verwaltung eingehender und ausgehender E-Mails.

Themen in diesem Kapitel:

9.1 Haftungsausschlüsse **232**

9.2 Automatische Antworten **236**

9.3 Listenserver **238**

9.4 E-Mail-Überwachung **243**

9.1 Haftungsausschlüsse

Haftungsausschlüsse sind Standardinhalte, die aus rechtlichen Gründen und/oder zu Marketing-Zwecken an das Ende oder den Anfang ausgehender E-Mails gestellt werden. Sie helfen Unternehmen, sich vor den potenziellen rechtlichen Folgen abzusichern, die durch den Missbrauch von Firmen-E-Mails entstehen können, und können verwendet werden, um Beschreibungen zu angebotenen Produkten/Services hinzuzufügen.

» Konfigurieren von Haftungsausschlüssen

» Deaktivieren und Aktivieren von Haftungsausschlüssen

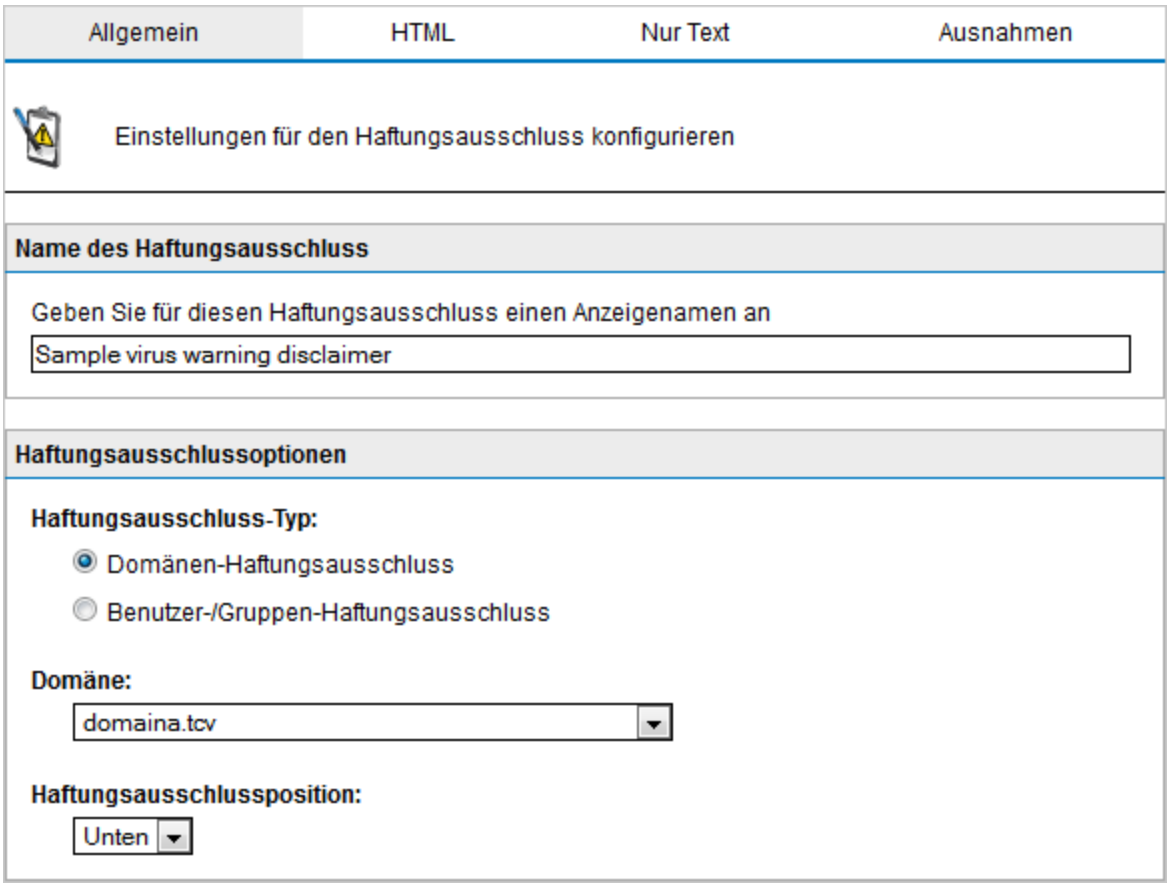
» Sortieren von Haftungsausschlüssen nach Priorität

9.1.1 Konfigurieren von Haftungsausschlüssen

So erstellen Sie einen neuen Haftungsausschluss oder passen ihn an:

1. Öffnen Sie **E-Mail-Verwaltung > Haftungsausschlüsse**.

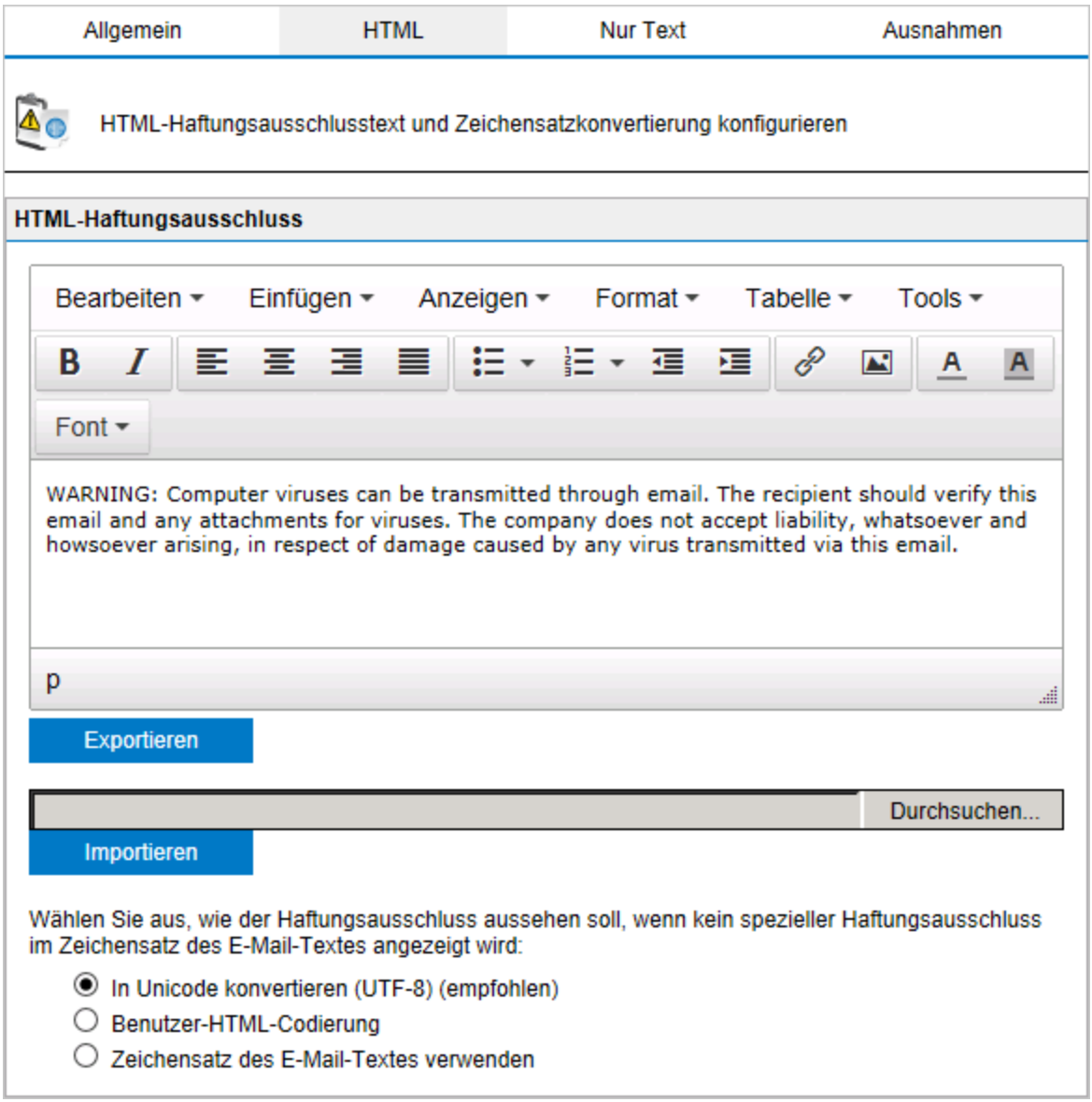
2. Klicken Sie auf einen Haftungsausschluss, um dessen Einstellungen zu bearbeiten. Oder klicken Sie auf **Haftungsausschluss hinzufügen**, um einen neuen Haftungsausschluss zu erstellen.



Screenshot 121: Hinzufügen eines neuen Haftungsausschlusses

3. Konfigurieren Sie auf der Registerkarte **Allgemein** Folgendes:

Option	Beschreibung
Name des Haftungsausschlusses	Geben Sie einen eindeutigen Anzeigenamen für den Haftungsausschluss ein.
Haftungsausschluss-Typ	Wählen Sie, für welche Benutzer dieser Haftungsausschluss angewendet wird: » **Domänen-Haftungsausschluss**: Alle von einer Domäne verschickten E-Mails werden mit dem Haftungsausschluss versehen. Wählen Sie die Domäne aus der Dropdown-Liste **Domäne** aus. » **Benutzer-/Gruppen-Haftungsausschluss**: Klicken Sie auf **Benutzer/Gruppe suchen**, um einen Benutzer oder eine Gruppe auszuwählen, bei dem/der der Haftungsausschluss in ausgehenden E-Mails hinzugefügt werden soll. Befindet sich GFI MailEssentials im Active Directory-Modus, wählen Sie die Benutzer oder Gruppen direkt in Active Directory aus. Geben Sie andernfalls die SMTP-E-Mail-Adressen der Benutzer an.
Haftungsausschluss - Position	Wählen Sie **Oben** oder **Unten** aus, um festzulegen, ob der Haftungsausschluss am Anfang oder am Ende der E-Mail angezeigt werden soll.


Allgemein
HTML
Nur Text
Ausnahmen
HTML-Haftungsausschlusstext und Zeichensatzkonvertierung konfigurieren
HTML-Haftungsausschluss
Bearbeiten
Einfügen
Anzeigen
Format
Tabelle
Tools
Font
WARNING: Computer viruses can be transmitted through email. The recipient should verify this email and any attachments for viruses. The company does not accept liability, whatsoever and howsoever arising, in respect of damage caused by any virus transmitted via this email.
p
Exportieren
Durchsuchen...
Importieren
Wählen Sie aus, wie der Haftungsausschluss aussehen soll, wenn kein spezieller Haftungsausschluss im Zeichensatz des E-Mail-Textes angezeigt wird:
In Unicode konvertieren (UTF-8) (empfohlen)
Benutzer-HTML-Codierung
Zeichensatz des E-Mail-Textes verwenden

Screenshot 122: HTML-Haftungsausschluss

4. Verwenden Sie auf der Registerkarte **HTML** den HTML-Editor, um einen benutzerdefinierten Haftungsausschluss im HTML-Format zu erstellen. Um E-Mail-Felder oder Active Directory-Felder (Variablen) in den Haftungsausschluss einzufügen, öffnen Sie **Einfügen > Variable...**. Wählen Sie die gewünschte Variable aus, und klicken Sie auf **Hinzufügen**.

> **HINWEIS**
>
> Die Variablen für den Anzeigenamen und die E-Mail-Adresse des Empfängers werden nur dann eingesetzt, wenn die E-Mail lediglich an einen einzelnen Empfänger geschickt wird. Beim Verschicken von E-Mails an mehrere Empfänger werden die Variablen automatisch mit dem Eintrag 'Empfänger' ersetzt.

5. Wählen Sie die Codierung für den HTML-Haftungsausschluss aus, wenn der Zeichensatz des E-Mail-Texts nicht HTML ist:

Option	Beschreibung
In Unicode konvertieren	E-Mail-Text und Haftungsausschluss werden in Unicode konvertiert, so dass beide ordnungsgemäß angezeigt werden. (Empfohlen)

Option	Beschreibung
HTML-Codierung verwenden	Mit dieser Option können Sie Zeichensätze für den E-Mail-Text und den Haftungsausschluss definieren.
Zeichensatz des E-Mail-Texts verwenden	Der Haftungsausschluss wird in den Zeichensatz des E-Mail-Texts konvertiert. **HINWEIS:** Bei Auswahl dieser Option wird möglicherweise nicht der ganze Haftungsausschlusstext ordnungsgemäß angezeigt.

6. Wählen Sie die Registerkarte **Nur Text** aus, und fügen Sie direkt im Feld **Haftungsausschlusstext** den Text ein, der für E-Mails im „Nur Text“-Format verwendet werden soll. Sie können im Haftungsausschluss Variablen hinzufügen, indem Sie auf **Variable…** klicken. Die Variablen, die hinzugefügt werden können, sind E-Mail- (Absendername, E-Mail-Adresse des Empfänger usw.) oder Active Directory-Felder (Name, Titel, Telefonnummern usw.). Wählen Sie die gewünschte Variable aus, und klicken Sie auf **Hinzufügen**.

> **HINWEIS**
>
> Die Variablen für den Anzeigenamen und die E-Mail-Adresse des Empfängers werden nur dann eingesetzt, wenn die E-Mail lediglich an einen einzelnen Empfänger geschickt wird. Beim Verschicken von E-Mails an mehrere Empfänger werden die Variablen automatisch mit dem Eintrag 'Empfänger' ersetzt.

7. Legen Sie die Codierung für den „Nur Text“-Haftungsausschluss fest, wenn der Zeichensatz des E-Mail-Texts nicht „Nur Text“ ist:

Option	Beschreibung
In Unicode konvertieren	E-Mail-Text und Haftungsausschluss werden in Unicode konvertiert, so dass beide ordnungsgemäß angezeigt werden.
Zeichensatz des E-Mail-Texts verwenden	Der Haftungsausschluss wird in den Zeichensatz des E-Mail-Texts konvertiert. **HINWEIS:** Bei Auswahl dieser Option wird möglicherweise nicht der ganze Haftungsausschlusstext ordnungsgemäß angezeigt.

8. Auf der Registerkarte **Ausnahmen** können Sie Absender oder Empfänger festlegen, auf die dieser Haftungsausschluss nicht angewendet werden soll. Geben Sie eine E-Mail-Adresse ein, oder klicken Sie auf **Suche**, um E-Mail-Adressen aus dem Active Directory auszuwählen. Klicken Sie auf **Hinzufügen**, um der Ausnahmeliste E-Mail-Adressen hinzuzufügen.

> **HINWEIS**
>
> Alle Empfänger müssen in die Ausschlussliste aufgenommen werden, damit E-Mails kein Haftungsausschluss hinzugefügt wird.

9. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

Siehe auch:

» Deaktivieren und Aktivieren von Haftungsausschlüssen

» Sortieren von Haftungsausschlüssen nach Priorität

9.1.2 Deaktivieren und Aktivieren von Haftungsausschlüssen

Haftungsausschlüsse werden standardmäßig automatisch aktiviert. So können Sie einen Haftungsausschluss deaktivieren oder aktivieren:

1. Öffnen Sie **E-Mail-Verwaltung > Haftungsausschlüsse**.

2. Wählen Sie die zu aktivierenden/deaktivierenden Haftungsausschlüsse aus, und klicken Sie auf **Auswahl deaktivieren** oder **Auswahl aktivieren**, um die gewünschte Aktion auszuführen.

Siehe auch:

» Konfigurieren von Haftungsausschlüssen

» Sortieren von Haftungsausschlüssen nach Priorität

9.1.3 Sortieren von Haftungsausschlüssen nach Priorität

Die Reihenfolge, in der Haftungsausschlüsse auf ausgehende E-Mails angewendet werden, kann angepasst werden. Wenn mehrere Haftungsausschlüsse aktiviert sind und auf den gleichen Benutzer angewendet werden, wird der Haftungsausschluss mit der höheren Priorität verwendet.

So passen Sie die Priorität von Haftungsausschlüssen an:

1. Öffnen Sie **E-Mail-Verwaltung > Haftungsausschlüsse**.

2. Klicken Sie zum Ändern der Priorität neben dem Haftungsausschluss auf ↑ (nach oben), um ihm eine höhere Priorität zuzuweisen, oder auf ↓ (nach unten), um ihm eine niedrigere Priorität zuzuweisen.

Siehe auch:

» Konfigurieren von Haftungsausschlüssen

» Deaktivieren und Aktivieren von Haftungsausschlüssen

9.2 Automatische Antworten

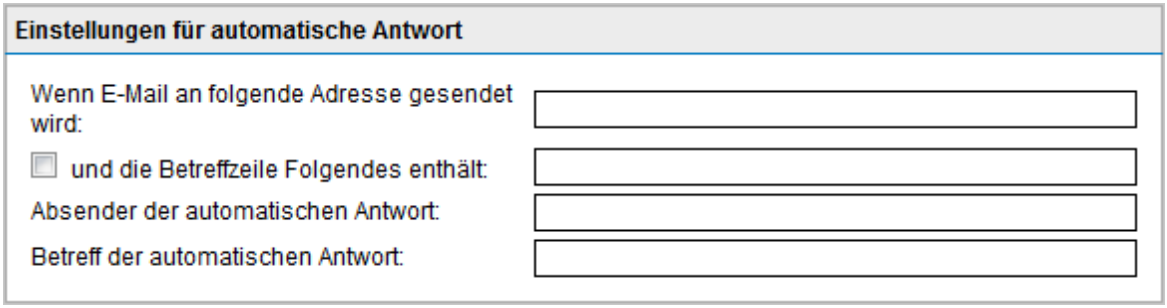
Mit dieser Funktion können automatische Antworten an bestimmte eingehende E-Mails gesendet werden. Dabei kann für jede E-Mail-Adresse oder jeden Betreff eine andere automatische Antwort definiert werden. Zur Personalisierung von E-Mails können Variablen in der automatischen Antwort verwendet werden.

Um automatische Antworten zu aktiveren, öffnen Sie **E-Mail-Verwaltung > Automatische Antworten**, und wählen Sie **Automatische Antworten aktivieren**.

9.2.1 Konfigurieren von automatischen Antworten

1. Öffnen Sie **E-Mail-Verwaltung > Automatische Antworten**.

2. Klicken Sie auf **Automatische Antwort hinzufügen**.


Einstellungen für automatische Antwort
Wenn E-Mail an folgende Adresse gesendet wird:
und die Betreffzeile Folgendes enthält:
Absender der automatischen Antwort:
Betreff der automatischen Antwort:

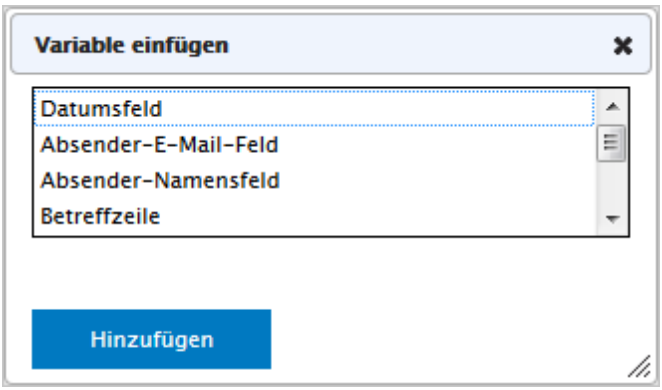
Screenshot 123: Einstellungen für automatische Antwort

3. Konfigurieren Sie unter **Einstellungen für automatische Antwort** die folgenden Optionen:

Option	Beschreibung
Wenn E-Mail an folgende Adresse gesendet wird:	Geben Sie die E-Mail-Adresse ein, von der beim Empfang von E-Mails automatische Antworten gesendet werden sollen. **Beispiel:** Wenn Sie „sales@master-domain.com“ eingeben, erhalten Personen, die eine E-Mail an diese Adresse senden, eine automatische Antwort.
und Betreff enthält:	Diese Option aktiviert die automatischen Antworten nur für E-Mails, die im Betrefffeld einen bestimmten Wortlaut enthalten.
Absender der automatischen Antwort:	Geben Sie eine E-Mail-Adresse an, wenn die automatische Antwort von einer anderen Adresse gesendet werden soll – also nicht von der Adresse, an die die eingehende E-Mail adressiert war.
Betreff der automatischen Antwort:	Geben Sie den Betreff der automatischen Antwort-E-Mail an.

4. Geben Sie im Feld **Text der automatischen Antwort** den Text der automatischen Antwort-E-Mail ein.

> **HINWEIS**
>
> Mit der Schaltfläche **Importieren** können Sie einen Text für die automatische Antwort aus einer Textdatei importieren. Klicken Sie auf **Exportieren**, um Text für eine automatische Antwort in eine Textdatei zu exportieren.



Screenshot 124: Dialogfeld für Variablen

5. Klicken Sie auf **Variable…**, um automatische Antworten mit Variablen zu personalisieren. Wählen Sie das einzufügende Variablenfeld aus, und klicken Sie auf **OK**. Folgende Variablen sind verfügbar:

Option	Beschreibung
Datumsfeld	Fügt das E-Mail-Absendedatum ein.
Absender-E-Mail-Feld	Fügt die E-Mail-Adresse des Absenders ein.
Absender-Namensfeld	Fügt den Anzeigenamen des Absenders ein.
Betreffzeile	Fügt den E-Mail-Betreff ein.
Empfänger-E-Mail-Feld	Fügt die E-Mail-Adresse des Empfängers ein.
Empfänger-Namensfeld	Fügt den Anzeigenamen des Empfängers ein.
Referenznummer	Fügt die Referenznummer ein (falls erstellt).

6. Wählen Sie im Bereich **Anhänge** die Anhänge, die mit der automatischen Antwort-E-Mail mitgeschickt werden sollen. Geben Sie den Speicherort für den Anhang an, und klicken Sie auf **Hinzufügen**. Zum Entfernen von Anhängen klicken Sie auf **Entfernen**.

7. Konfigurieren Sie Folgendes unter **Sonstige Einstellungen**:

Option	Beschreibung
Referenznummer in der Betreffzeile generieren	Erzeugt eine einzigartige Referenznummer in der automatischen Antwort. Referenznummern werden standardmäßig im folgenden Format generiert: `ME_JJMMTT_nnnnnn` Bedeutung der Parameter: » `ME` - GFI MailEssentials-Tag. » `JJMMTT` - Das Datum (Jahr, Monat, Tag). » `nnnnnn` - Die automatisch generierte Referenznummer.
Gesendete E-Mails einschließen	Wählen Sie diese Option, um die eingegangene E-Mail in die automatische Antwort einzuschließen.

8. Klicken Sie auf **Übernehmen**.

9.3 Listenserver

Listen-Server ermöglichen die Erstellung zweier Arten von Verteilerlisten:

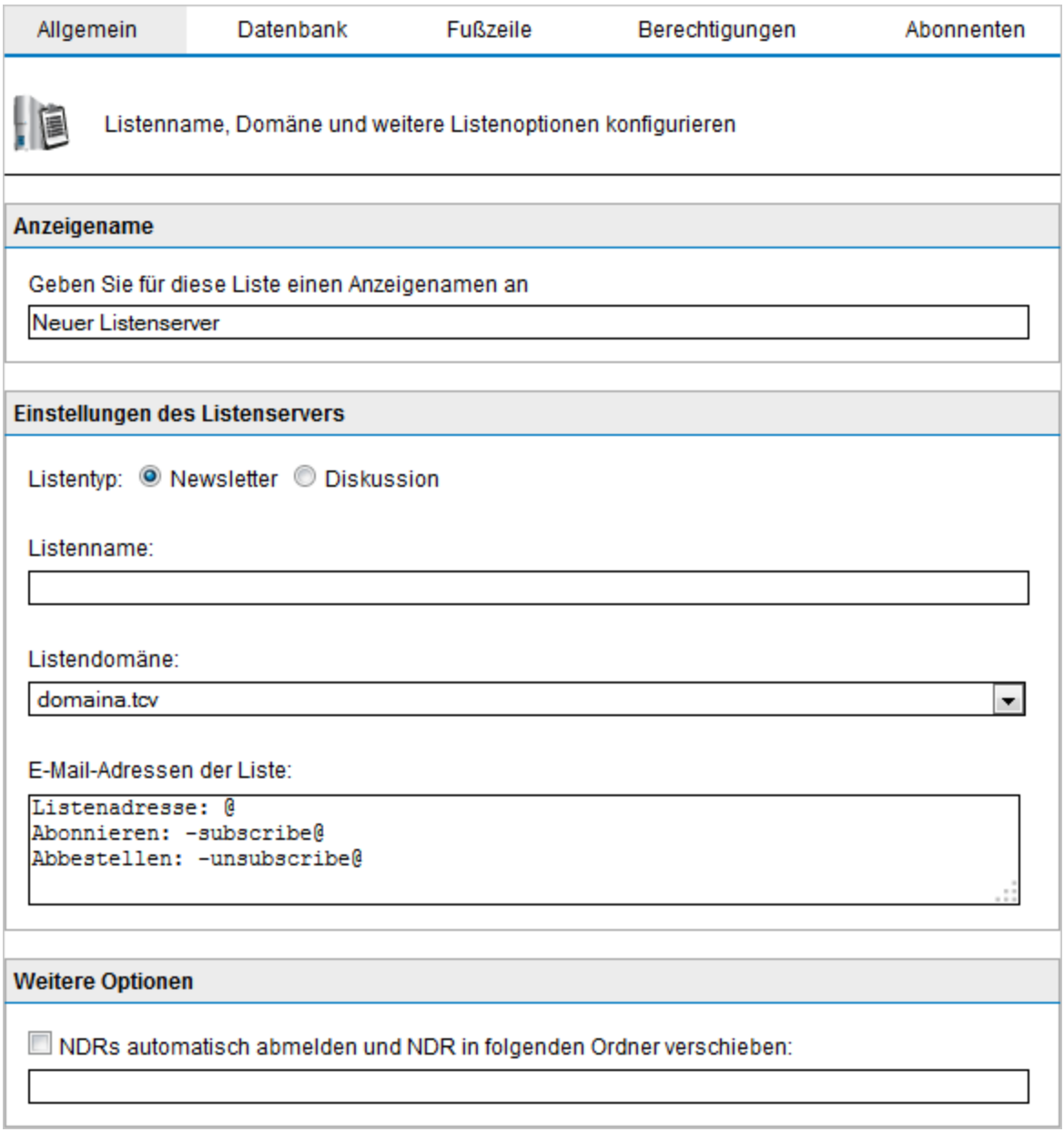
» **Newsletter** – Wird zur Erstellung von Abonnementlisten für Unternehmens- oder Produkt-Newsletter verwendet, die von den Benutzern abonniert oder abbestellt werden können.

» **Diskussion** – Ermöglicht es einer Gruppe von Teilnehmern, eine Diskussion per E-Mail zu führen. Jeder Abonnent der Liste erhält alle E-Mails, die an diese Liste geschickt werden.

9.3.1 Erstellen eines Newsletters oder einer Diskussionsliste

So erstellen Sie einen neuen Newsletter oder eine neue Diskussionsliste:

1. Öffnen Sie **E-Mail-Verwaltung > Listenserver**, und klicken Sie auf **Liste hinzufügen**.



Screenshot 125: Erstellen einer neuen Liste

2. Konfigurieren Sie die folgenden Optionen:

Option	Beschreibung
Anzeigename	Geben Sie einen Anzeigenamen für die neue Liste ein.
Listentyp	Wählen Sie den Typ der zu erstellenden Diskussionsliste aus: » **Newsletter** - Wird zur Erstellung von Abonnementlisten für Unternehmens- oder Produkt-Newsletter verwendet, die von den Benutzern abonniert oder abbestellt werden können. » **Diskussion** - Ermöglicht es einer Gruppe von Teilnehmern, eine Diskussion per E-Mail zu führen. Jeder Abonnent der Liste erhält alle E-Mails, die an diese Liste geschickt werden.
Namen auflisten	Der Listenname wird in den Feldern der Listen-E-Mail-Adresse verwendet. Wenn der Listenname beispielsweise `MeinNewsletter` lautet, ist die Listen-E-Mail-Adresse `MeinNewsletter@mydomain.com`.

Option	Beschreibung
Listendomäne	Die für die Liste zu verwendende Domäne. Die Liste der Domänen wird aus der Liste Lokale Domänen extrahiert. Der Listenserver verwendet diese Domäne für die Listenadressen, in im Feld **Listen-E-Mail-Adressen** angezeigt werden.
NDRs automatisch abmelden und NDR in folgenden Ordner verschieben:	Wenn von einem Abonnenten der Liste ein NDR empfangen wird, wird der Abonnent automatisch ausgetragen und der NDR in einen benutzerdefinierten Ordner verschoben.

3. Wählen Sie auf der Registerkarte **Datenbank** die Option **Microsoft Access** oder **Microsoft SQL Server/MSDE** als Datenbank aus. Konfigurieren Sie den ausgewählten Datenbanktyp zum Speichern der Abonnentenliste für den Newsletter bzw. die Diskussionsliste. Folgende Optionen sind verfügbar:

Option	Beschreibung
Microsoft Access	Geben Sie einen Datenbanknamen und -speicherort an. GFI MailEssentials erstellt automatisch eine Datenbank.
Microsoft SQL Server	Geben Sie den SQL-Servernamen, die Datenbank und die verwendeten Anmeldeinformationen an, um die Abonnentenliste für den Newsletter/die Diskussionsliste zu speichern. Klicken Sie auf „Test“, um sicherzustellen, dass sich GFI MailEssentials mit dem angegebenen Microsoft SQL Server verbinden kann.

> **HINWEIS**
>
> Für Listen mit bis zu 5.000 Abonnenten können Sie Microsoft Access verwenden.

4. Passen Sie Ihre Verteilerliste an. Weitere Informationen finden Sie unter „Konfigurieren erweiterter Eigenschaften für Newsletter/Diskussionslisten“ (Seite 241).

5. Klicken Sie auf **Übernehmen**.

9.3.2 Verwenden von Newslettern/Diskussionen

Nachdem ein Newsletter oder eine Diskussionsliste erstellt wurde, müssen die Benutzer sie abonnieren, um an der Liste teilzunehmen.

Aktion	Beschreibung
Liste abonnieren	Die Benutzer müssen eine E-Mail an folgende Adresse senden: `<Newslettername>-subscribe@ihredomäne.com`
Abonnement abschließen	Sobald der Listenserver die Anfrage erhält, sendet er eine Bestätigungs-E-Mail zurück. Die Benutzer müssen ihr Abonnement mit einer Antwort-E-Mail bestätigen, um als Abonnent hinzugefügt zu werden. **HINWEIS:** Der Versand der Bestätigungs-E-Mail ist eine Voraussetzung, die nicht deaktiviert werden kann.
Newsletter-/Diskussionsbeitrag senden	Mitglieder, die berechtigt sind, E-Mails an die Liste zu schicken, senden diese an die E-Mail-Adresse der Newsletter-Liste: `<Newslettername>@ihredomäne.com`
Liste abbestellen	Um die Liste abzubestellen, müssen die Benutzer eine E-Mail an folgende Adresse schicken: `<Newslettername>-unsubscribe@ihredomäne.com`

> **HINWEIS**
>
> Sie können das Abonnieren von Newslettern für die Benutzer vereinfachen, indem Sie ein Webformular zum Eingeben von Name und E-Mail-Adresse hinzufügen und automatisch eine E-Mail generieren, die als Absender die E-Mail-Adresse des neuen Benutzers und als Empfänger folgende Adresse enthält:
>
> `<Newslettername>-subscribe@ihredomäne.com`

9.3.3 Konfigurieren erweiterter Eigenschaften für Newsletter/Diskussionslisten

Nachdem Sie eine neue Liste erstellt haben, können Sie weitere Optionen konfigurieren, um die Elemente und das Verhalten der Liste anzupassen. Folgende Optionen sind verfügbar:

- Erstellen einer Listen-spezifischen Fußzeile
- Einrichten von Listen-spezifischen Berechtigungen
- Manuelles Hinzufügen neuer Abonnenten
- Importieren von Abonnenten in die Liste/Datenbankstruktur

Erstellen einer Listen-spezifischen Fußzeile

1. Konfigurieren Sie auf der Registerkarte **Fußzeile** eine benutzerdefinierte Fußzeile für Diskussionslisten. Die Fußzeile wird jeder E-Mail hinzugefügt, die an die Liste gesendet wird.

2. Verwenden Sie den HTML-Editor, um einen HTML-Version der Fußzeile hinzuzufügen. Um Variablenfelder in die Listenfußzeile einzufügen, öffnen Sie **Einfügen > Variable**. Wählen Sie die gewünschte Variable aus, und klicken Sie auf **Liste hinzufügen**.

3. Sie können auch eine Nur-Text-Fußzeile für Nur-Text-Listen eingeben. Klicken Sie auf **Variable...**, um Variablenfelder hinzuzufügen.

4. Klicken Sie auf **Übernehmen**.

> **Tipp**
>
> Sie können Fußzeilen verwenden, um zu zeigen, wie Anwender die Liste abonnieren und wieder abbestellen und ihre Kanäle in sozialen Medien bewerben.

Einrichten von Newsletter-spezifischen Berechtigungen

Geben Sie die Benutzer an, die Newsletter verschicken können.

> **HINWEIS**
>
> Für Diskussionslisten sind keine Berechtigungen konfigurierbar.

1. Öffnen Sie eine vorhandene Liste oder erstellen Sie eine neue, und öffnen Sie die Registerkarte **Berechtigungen**.

2. Geben Sie eine E-Mail-Adresse ein, von der Newsletter verschickt werden können, und klicken Sie auf **E-Mail hinzufügen**. Die angegebene E-Mail-Adresse wird der Liste hinzugefügt.

3. Ein Newsletter-Kennwort sichert den Zugriff auf Newsletter, falls der E-Mail-Client oder die Kontodaten eines zugriffsberechtigten Anwenders auch von anderen Benutzern verwendet werden. Aktivieren Sie die Verwendung von Kennwörtern, indem Sie das Kontrollkästchen **Kennwort erforderlich** auswählen und ein Kennwort eingeben.

HINWEIS

Die Benutzer müssen sich durch Angabe des Kennworts in der E-Mail-Betreffzeile authentifizieren, um Nachrichten an die Newsletter-Liste schicken zu können. Das Kennwort muss im Betreff wie folgt angegeben werden:

`[PASSWORD:<Kennwort>] <Betreff der E-Mail>`

Beispiel: `[PASSWORD:darf_posten] Sonderaktion`

Ist das Kennwort korrekt, entfernt der Listenserver automatisch die Kennwortinformationen aus dem Betreff und leitet die E-Mail an den Newsletter-Abonnenten weiter.

4. Klicken Sie auf **Übernehmen**.

Manuelles Hinzufügen neuer Abonnenten

Sie können Benutzer manuell zu Newslettern/Diskussionen hinzufügen, wobei keine Aktion durch die Benutzer selbst erforderlich ist.

HINWEIS

Es wird dringend empfohlen, dass die Benutzer ihre gewünschten Listen selbst abonnieren, indem sie eine E-Mail an die Anmeldeadresse des Newsletters bzw. der Diskussionsliste senden. Stellen Sie sicher, dass Sie die Zustimmung eines Benutzers einholen, bevor Sie ihn manuell einer Liste hinzufügen.

1. Öffnen Sie eine vorhandene Liste oder erstellen Sie eine neue, und öffnen Sie die Registerkarte **Abonnenten**.

2. Geben Sie die Abonnenteninformationen in die Felder **E-Mail-Adresse** (erforderlich), **Vorname**, **Nachname** und **Unternehmen**, und klicken Sie auf **E-Mail hinzufügen**. Die E-Mail-Adresse des neuen Abonnenten wird der Liste hinzugefügt.

3. Sollen Benutzer bei Beendigung des Abonnements komplett aus der Abonnentenliste gelöscht werden (und nicht nur als inaktiv gekennzeichnet), aktivieren Sie das Kontrollkästchen **Bei Abmeldung des Benutzers aus Datenbank löschen**.

4. Klicken Sie auf **Übernehmen**.

Importieren von Abonnenten in die Liste/Datenbankstruktur

Wenn Sie einen neuen Newsletter oder eine neue Diskussionsliste erstellt haben, wird eine Tabelle mit dem Namen 'listname_subscribers' in der Datenbank erstellt, die die unten stehenden Felder enthält.

Sollen Daten in die Liste importiert werden, füllen Sie die folgenden Felder der Datenbank aus.

Feldname	Typ	Standardwert	Kennzeichnungen	Beschreibung
Ls_id	Varchar(100)		PK	Abonnenten-ID
Ls_first	Varchar(250)			Vorname
Ls_last	Varchar(250)			Nachname
Ls_email	Varchar(250)			E-Mail
Ls_unsubscribed	Int	0	NOT NULL	Abbestellungskennzeichen
Ls_company	Varchar(250)			Unternehmensname

9.4 E-Mail-Überwachung

Mithilfe der E-Mail-Überwachung können Sie E-Mails kopieren, die an eine oder von einer bestimmten lokalen E-Mail-Adresse an eine andere E-Mail-Adresse gesendet werden. Dadurch lässt sich der E-Mail-Verkehr einer Person oder Abteilung zentral speichern.

9.4.1 Hinzufügen neuer E-Mail-Überwachungsregeln

1. Öffnen Sie **E-Mail-Verwaltung > E-Mail-Überwachung**.

2. Klicken Sie auf **Regel hinzufügen...**.

3. Konfigurieren Sie auf der Registerkarte **Allgemein** die folgenden Optionen:

Option	Beschreibung
E-Mail-Überwachungsname	Geben Sie einen Anzeigenamen für die E-Mail-Überwachungsregel ein.
Eingehend oder **ausgehend**	Wählen Sie, ob die Regel auf eingehende oder ausgehende E-Mails angewendet werden soll.
Überwachte E-Mail in Benutzer/E-Mail-Adresse kopieren	Die Ziel-E-Mail-Adresse bzw. das Zielpostfach an, in das die E-Mails kopiert werden sollen. Wählen Sie **E-Mail-Adresse**, um manuell eine E-Mail-Adresse einzugeben, oder wählen Sie **Benutzer**, um danach zu suchen.
Wenn Absender	Geben Sie die E-Mail-Adresse des zu überwachenden Absenders ein. Klicken Sie auf **Alle Domänen**, um die gesendeten E-Mails aller Benutzer zu überwachen.
und Empfänger	Geben Sie die E-Mail-Adresse des zu überwachenden Empfängers ein. Klicken Sie auf **Alle Domänen**, um die empfangenen E-Mails aller Benutzer zu überwachen.

4. Klicken Sie auf **Hinzufügen**, um die konfigurierte Regel hinzuzufügen.

5. Wiederholen Sie die obigen Schritte, um mehrere Filter anzugeben.

6. Geben Sie auf der Registerkarte **Ausnahmen** die Benutzer und E-Mail-Adressen an, auf die die Regel nicht angewendet werden soll. Folgende Optionen sind verfügbar:

Option	Beschreibung
Außer wenn Absender	Schließt die angegebenen Absender von der E-Mail-Überwachung aus. Geben Sie für Überwachungsregeln für eingehende E-Mails die nicht lokalen E-Mail-Adressen ein. Für Überwachungsregeln für ausgehende Regeln sind alle Adressen in dieser Liste lokal. Klicken Sie auf **Benutzer suchen**, um nach lokalen E-Mail-Adressen zu suchen, und klicken Sie auf **Hinzufügen**.
Außer wenn Empfänger	Schließt die angegebenen Empfänger aus der Liste aus. Für Überwachungsregeln für eingehende Regeln sind alle Adressen in dieser Liste lokal. Klicken Sie auf **Benutzer suchen**, um nach lokalen E-Mail-Adressen zu suchen, und klicken Sie auf **Hinzufügen**. Geben Sie für die Überwachungsregel für ausgehende E-Mails die nicht lokalen E-Mail-Adressen ein.

7. Klicken Sie auf **Übernehmen**.

9.4.2 So verwenden Sie die E-Mail-Überwachung

Informationen zur Konfiguration der E-Mail-Überwachung für unterschiedliche Anforderungen und Szenarien finden Sie in der nachfolgenden Tabelle:

Zu überwachendes Element	Beschreibung
Alle E-Mails, die von einem bestimmten Benutzer gesendet werden	Erstellen Sie eine Regel für ausgehende E-Mails, und geben Sie die E-Mail-Adresse des Absenders an oder suchen Sie im Absenderfeld nach dem Benutzer (bei Verwendung von AD). Klicken Sie im Empfängerfeld auf **Alle Domänen**.
Alle E-Mails, die an einen bestimmten Benutzer gesendet werden	Erstellen Sie eine Regel für eingehende E-Mails, und geben Sie die E-Mail-Adresse des Empfängers an oder suchen Sie im Empfängerfeld nach dem Benutzer (bei Verwendung von AD). Klicken Sie im Absenderfeld auf **Alle Domänen**.

Zu überwachendes Element	Beschreibung
E-Mails, die von einem bestimmten Benutzer an einen externen Empfänger gesendet werden	Erstellen Sie eine Regel für ausgehende E-Mails, indem Sie im Absenderfeld den Absender eingeben oder den Benutzer auswählen (bei Verwendung von AD). Geben Sie die E-Mail-Adresse des externen Empfängers im Empfängerfeld ein.
E-Mails, die von einem externen Absender an einen bestimmten Benutzer gesendet werden	Erstellen Sie eine Regel für eingehende E-Mails, und geben Sie im Absenderfeld die E-Mail-Adresse des externen Absenders ein. Geben Sie die E-Mail-Adresse ein oder wählen Sie den Benutzer im Empfängerfeld aus (bei Verwendung von AD).
E-Mails, die von einem bestimmten Benutzer an ein Unternehmen oder eine Domäne gesendet werden	Erstellen Sie eine Regel für ausgehende E-Mails, indem Sie im Absenderfeld den Absender eingeben oder den Benutzer auswählen (bei Verwendung von AD). Geben Sie die Domäne des Unternehmens im Empfängerfeld an.
E-Mails, die von einem Unternehmen oder einer Domäne an einen bestimmten Benutzer gesendet werden	Erstellen Sie eine Regel für eingehende E-Mails, und geben Sie im Absenderfeld die Domäne des Unternehmens an. Wählen Sie die Domäne durch Klicken auf die Absenderschaltfläche aus, und geben Sie im Empfängerfeld den betreffenden Benutzernamen oder die E-Mail-Adresse des Benutzers ein.

9.4.3 Aktivieren/Deaktivieren der E-Mail-Überwachungsregeln

1. Öffnen Sie **E-Mail-Verwaltung > E-Mail-Überwachung**.

2. Wählen Sie die zu aktivierende/zu deaktivierende Regel aus.

3. Klicken Sie auf **Auswahl aktivieren** oder **Auswahl deaktivieren**, um die ausgewählte Regel zu aktivieren bzw. zu deaktivieren.

4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

10 Allgemeine Einstellungen

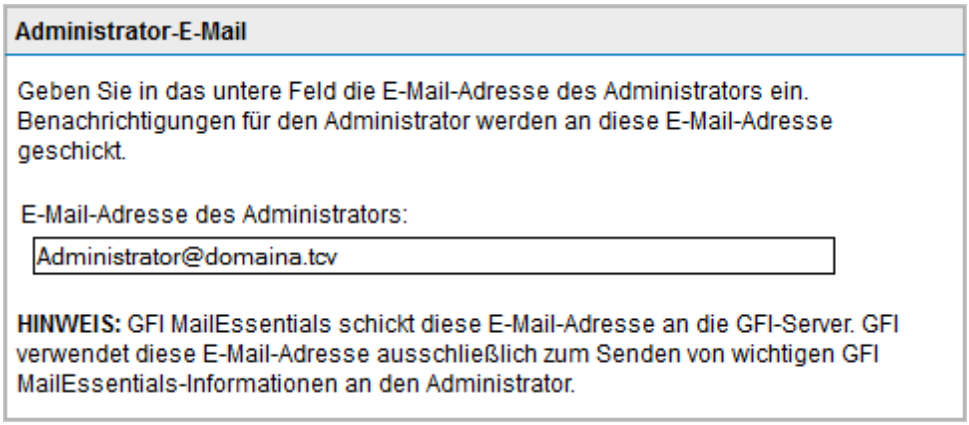
Themen in diesem Kapitel:

10.1 Administrator-E-Mail-Adresse 245
10.2 Aktivieren/Deaktivieren von Scan-Modulen 245
10.3 Proxy-Einstellungen 246
10.4 Lokale Domänen 248
10.5 Verwalten lokaler Benutzer 249
10.6 Lizenzierung 250
10.7 Bindungen an virtuelle SMTP-Server 250
10.8 Patch-Überprüfung 250
10.9 Zugriffssteuerung 251

10.1 Administrator-E-Mail-Adresse

GFI MailEssentials sendet wichtige Benachrichtigungen per E-Mail an den Administrator. So richten Sie die Administrator-E-Mail-Adresse ein:

1. Wählen Sie in GFI MailEssentials Configuration die Optionen **Allgemeine Einstellungen > Einstellungen** und anschließend die Registerkarte **Allgemein** aus.


Administrator-E-Mail
Geben Sie in das untere Feld die E-Mail-Adresse des Administrators ein. Benachrichtigungen für den Administrator werden an diese E-Mail-Adresse geschickt.
E-Mail-Adresse des Administrators:
Administrator@domaina.tcv
HINWEIS: GFI MailEssentials schickt diese E-Mail-Adresse an die GFI-Server. GFI verwendet diese E-Mail-Adresse ausschließlich zum Senden von wichtigen GFI MailEssentials-Informationen an den Administrator.

Screenshot 126: Angeben der Administrator-E-Mail-Adresse

2. Geben Sie die Administrator-E-Mail-Adresse im Bereich **E-Mail-Adresse des Administrators** ein.

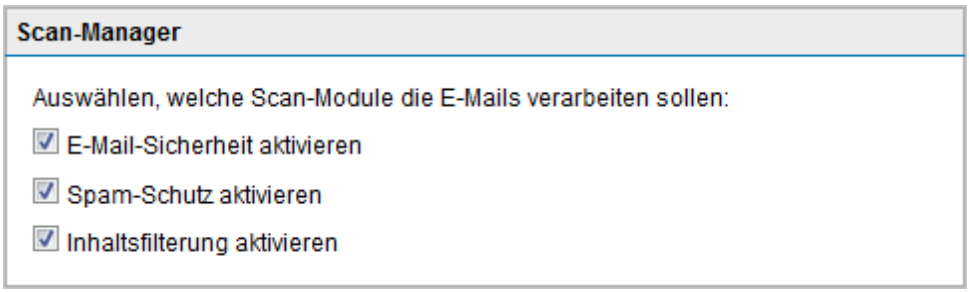
3. Klicken Sie auf **Übernehmen**.

10.2 Aktivieren/Deaktivieren von Scan-Modulen

Sie können in GFI MailEssentials bestimmte E-Mail-Scan-Module aktivieren oder deaktivieren. Auf diese Weise können Sie ganze Gruppen von Scan-Engines oder Filtern ein- und ausschalten.

> **HINWEIS**
>
> Mit dieser Funktion werden nur bestimmte Scan-Engines aktiviert oder deaktiviert. Deaktivierte Engines verarbeiten keine eingehenden, ausgehenden und/oder internen E-Mails. Alle anderen Funktionen von GFI MailEssentials, z. B. der Quarantänespeicher, bleiben aktiv.

1. Wählen Sie in GFI MailEssentials Configuration die Optionen **Allgemeine Einstellungen > Einstellungen** und anschließend die Registerkarte **Allgemein** aus.



Screenshot 127: Scan-Manager

2. Aktivieren oder deaktivieren Sie die gewünschten Scan-Module:

Option	Beschreibung
E-Mail-Sicherheit aktivieren	Aktiviert/deaktiviert die folgenden Scan-Engines: » Virenscan-Engines » Informationsspeicherschutz » Scanner für Trojaner und ausführbare Dateien » E-Mail-Exploit-Engine » HTML-Bereinigung
Spam-Schutz aktivieren	Aktiviert/deaktiviert die folgenden Anti-Spam-Filter: » SpamRazer » Anti-Phishing » Directory Harvesting » E-Mail-Blocklist » IP-Blocklist » IP-DNS-Blocklist » URI-DNS-Blocklist » Greylist » Spracherkennung » Bayes'sche Analyse » Whitelist » Neue Absender
Inhaltsfilterung aktivieren	Aktiviert/deaktiviert die folgenden Inhaltsfilter-Engines: » Stichwortfilterung » Anhangsfilterung » Dekomprimierungs-Engine » Erweiterte Inhaltsfilterung

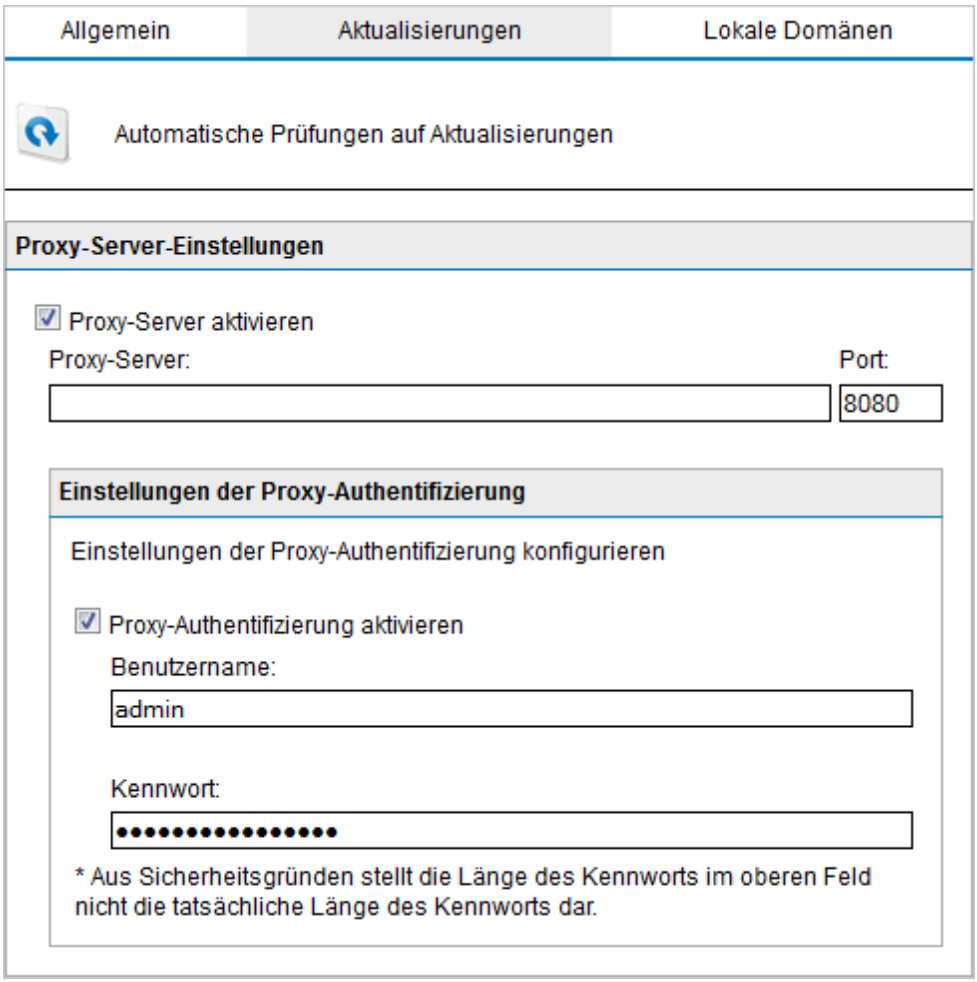
3. Klicken Sie auf **Übernehmen**.

10.3 Proxy-Einstellungen

GFI MailEssentials sucht im Internet automatisch nach Updates (z. B. für Virendefinitionen und SpamRazer-Definitionen) und lädt diese herunter. Wenn der Server, auf dem GFI MailEssentials

installiert ist, die Verbindung mit dem Internet über einen Proxy-Server herstellt, konfigurieren Sie die Proxy-Einstellungen wie folgt:

1. Wählen Sie in GFI MailEssentials Configuration die Optionen **Allgemeine Einstellungen** > **Einstellungen** und anschließend die Registerkarte **Aktualisierungen** aus.



Screenshot 128: Proxy-Einstellungen für den Aktualisierungsserver

2. Markieren Sie das Kontrollkästchen **Proxy-Server aktivieren**.

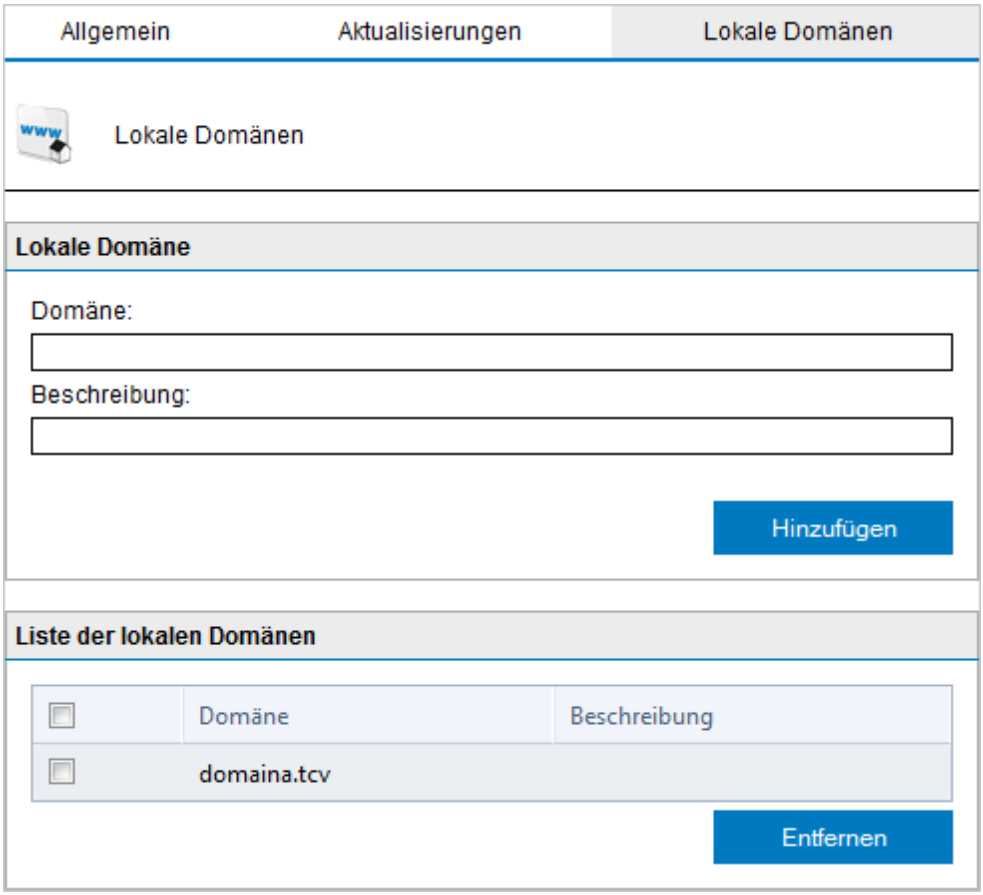
3. Geben Sie im Feld **Proxy-Server** den Namen oder die IP-Adresse des Proxy-Servers ein.

4. Geben Sie im Feld **Port** den Port ein, über den die Verbindung hergestellt werden soll (Standardwert ist 8080).

5. Falls der Proxy-Server eine Authentifizierung erfordert, wählen Sie **Proxy-Authentifizierung aktivieren** aus, und geben Sie den **Benutzernamen** und das **Kennwort** ein.

6. Klicken Sie auf **Übernehmen**.

10.4 Lokale Domänen



Screenshot 129: Liste der lokalen Domänen

GFI MailEssentials benötigt die Liste der lokalen Domänen, um zwischen eingehenden, ausgehenden und internen E-Mails unterscheiden zu können. Während der Installation oder im Nachinstallationsassistenten von GFI MailEssentials werden automatisch die lokalen Domänen vom IIS SMTP-Dienst oder Microsoft® Exchange Server importiert. In manchen Fällen müssen lokale Domänen jedoch manuell hinzugefügt werden.

WICHTIG

GFI MailEssentials filtert nur E-Mails, die an lokale Domänen gesendet werden, auf Spam. Auch einige Filterregeln basieren auf der Richtung des E-Mail-Verkehrs. Diese wird durch die lokalen Domänen bestimmt.

Führen Sie folgende Schritte aus, um nach der Installation lokale Domänen hinzuzufügen oder zu entfernen:

1. Wählen Sie **Allgemeine Einstellungen > Einstellungen** und anschließend die Registerkarte **Lokale Domänen** aus.

2. Geben Sie den Namen und die Beschreibung der hinzuzufügenden Domäne in den Textfeldern **Domäne** und **Beschreibung** ein.

3. Klicken Sie auf **Hinzufügen**, um die angegebene Domäne in die Liste **Lokale Domänen** aufzunehmen.

HINWEIS

Wählen Sie zum Entfernen einer Domäne diese aus der Liste aus, und klicken Sie auf **Entfernen**.

4. Klicken Sie auf **Übernehmen**.

10.5 Verwalten lokaler Benutzer

GFI MailEssentials kann Benutzer auf 3 Arten abrufen, abhängig von der jeweiligen Installationsumgebung.

HINWEIS

Die Anzahl der abgerufenen Benutzer wird auch für die Lizenzierung verwendet.

10.5.1 GFI MailEssentials ist im Active Directory-Modus installiert

Wenn GFI MailEssentials nicht auf demselben Rechner wie Ihr Mailserver installiert ist und Active Directory vorhanden ist, ruft GFI MailEssentials die E-Mail-Benutzer von der Active Directory-Domäne ab, zu der der GFI MailEssentials-Rechner gehört.

GFI MailEssentials ist auf dem Microsoft® Exchange-Rechner installiert

Ist GFI MailEssentials auf demselben Rechner wie Microsoft® Exchange installiert, ruft GFI MailEssentials die Active Directory-Benutzer ab, die ein Postfach auf diesem Microsoft® Exchange-Server haben.

10.5.2 GFI MailEssentials ist im SMTP-Modus installiert

Wenn Sie GFI MailEssentials im SMTP-Modus installieren, wird die Liste der lokalen Benutzer in einer Datenbank gespeichert, die von GFI MailEssentials verwaltet wird.

Wenn GFI MailEssentials im SMTP-Modus installiert ist, können Sie die Benutzerliste unter **Allgemein > Einstellungen** auf der Registerkarte **Benutzer-Manager** füllen und verwalten.

Die Registerkarte **Benutzer-Manager** zeigt die Liste der lokalen Benutzer und ermöglicht das Hinzufügen und Entfernen lokaler Benutzer. Die Liste der lokalen Benutzer wird zum Konfigurieren benutzerbasierter Regeln verwendet, z. B. für die **Anhangsfilterung** oder die **Inhaltsfilterung**.

HINWEIS

GFI MailEssentials füllt die Liste der lokalen Benutzer automatisch mithilfe der Absenderadressen ausgehender E-Mails.

So fügen Sie einen neuen lokalen Benutzer hinzu:

1. Geben Sie die E-Mail-Adresse im Feld **E-Mail-Adresse** ein.

2. Klicken Sie auf **Hinzufügen**.

3. Wiederholen Sie diesen Schritt, um weitere lokale Benutzer hinzuzufügen, und klicken Sie auf **Übernehmen**.

So entfernen Sie einen lokalen Benutzer:

1. Wählen Sie den lokalen Benutzer, den Sie entfernen möchten, in der Liste **Lokale Benutzer** aus, und klicken Sie auf **Entfernen**.

2. Wiederholen Sie diesen Schritt, um weitere lokale Benutzer zu entfernen, und klicken Sie auf **Übernehmen**.

10.6 Lizenzierung

Erwerben Sie eine Lizenz, die der Anzahl der von GFI MailEssentials zu schützenden Postfächer oder Benutzer entspricht.

Geben Sie den erworbenen Lizenzschlüssel während der Installation oder in der GFI MailEssentials-Konfiguration ein. Öffnen Sie **Allgemeine Einstellungen > Lizenzierung**, und geben Sie Ihren Lizenzschlüssel in das Feld **Lizenzschlüssel** ein. Klicken Sie auf **Übernehmen**.

Um Ihre Lizenzinformationen einschließlich des Ablaufdatums zu prüfen, öffnen Sie **Allgemeine Einstellungen > Lizenzierung**, und prüfen Sie die Details unter **Lizenzschlüsselinformationen**.

10.6.1 So bestimmen Sie die Lizenzanforderungen

GFI MailEssentials zählt die Gesamtpostfächer/-E-Mail-Adressen je nach Umgebung. Um die Anzahl der Benutzer in Ihrer Umgebung zu bestimmten, öffnen Sie http://go.gfi.com/?pageid=ME_RetrieveAndCountUsers.

10.7 Bindungen an virtuelle SMTP-Server

GFI MailEssentials wird immer an den ersten virtuellen SMTP-Server gebunden, der in IIS konfiguriert ist. Falls mehrere virtuelle SMTP-Server vorhanden sind, kann es erforderlich sein, dass GFI MailEssentials an einen neuen oder anderen virtuellen SMTP-Server gebunden wird.

> **HINWEIS**
>
> Die Registerkarte für Bindungen an virtuelle SMTP-Server wird nicht angezeigt, wenn Sie GFI MailEssentials auf einem Rechner mit Microsoft® Exchange Server 2007/2010 installiert haben.

10.7.1 GFI MailEssentials an einen anderen virtuellen SMTP-Server binden

> **HINWEIS**
>
> Einige Dienste werden vorübergehend angehalten, während dieser Vorgang ausgeführt wird. Dies kann den E-Mail-Fluss und/oder die E-Mail-Scans beeinträchtigen.

1. Wählen Sie **Allgemeine Einstellungen > Einstellungen** und anschließend die Registerkarte **Bindungen** aus.

2. Wählen Sie den virtuellen SMTP-Server aus, an den GFI MailEssentials gebunden werden soll.

3. Klicken Sie auf **Übernehmen**.

4. GFI MailEssentials fordert Sie auf, einen Dienste-Neustart durchzuführen, damit die neuen Einstellungen wirksam werden.

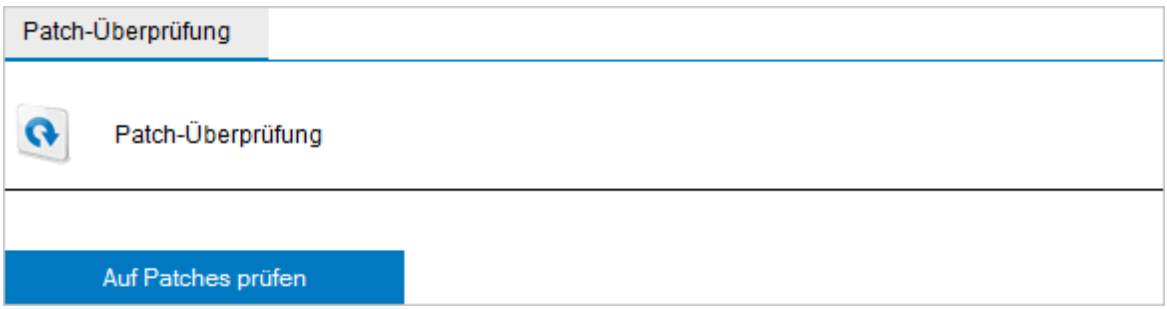
10.8 Patch-Überprüfung

Mit dieser Funktion wird geprüft, ob für Ihre Version von GFI MailEssentials Software-Patches zur Verfügung stehen. Dafür wird eine Verbindung mit den GFI-Aktualisierungsservern hergestellt.

HINWEIS

Es wird dringend empfohlen, regelmäßig nach Patches zu suchen, um GFI MailEssentials stets auf dem aktuellsten Stand zu halten.

1. Öffnen Sie **Allgemeine Einstellungen > Patch-Überprüfung**.



Screenshot 130: Prüfung auf Produkt-Patches

2. Klicken Sie auf **Auf Patches prüfen**, um eine Verbindung mit dem GFI-Aktualisierungsserver herzustellen und nach verfügbaren Updates zu suchen.

3. Klicken Sie auf den Link **Herunterladen** der Patches, die Sie herunterladen möchten.

4. Installieren Sie anschließend die heruntergeladenen Updates.

HINWEIS

Installationshinweise und andere Informationen zu einem Patch erhalten Sie durch Klicken auf den jeweiligen Informationslink in der Liste der verfügbaren Updates. Durch eine falsche Patch-Installation kann es zu Fehlfunktionen des Produkts oder zu Leistungseinbußen kommen.

10.9 Zugriffssteuerung

Sie können den Zugriff auf verschiedene Funktionen von GFI MailEssentials für bestimmte Domänenbenutzer oder Gruppen zulassen oder blockieren. Benutzer können mithilfe ihrer Domänenanmeldeinformationen auf die Weboberfläche von GFI MailEssentials zugreifen. Welche Funktionen den angemeldeten Benutzern angezeigt werden, hängt von der Konfiguration der Zugriffssteuerung ab.

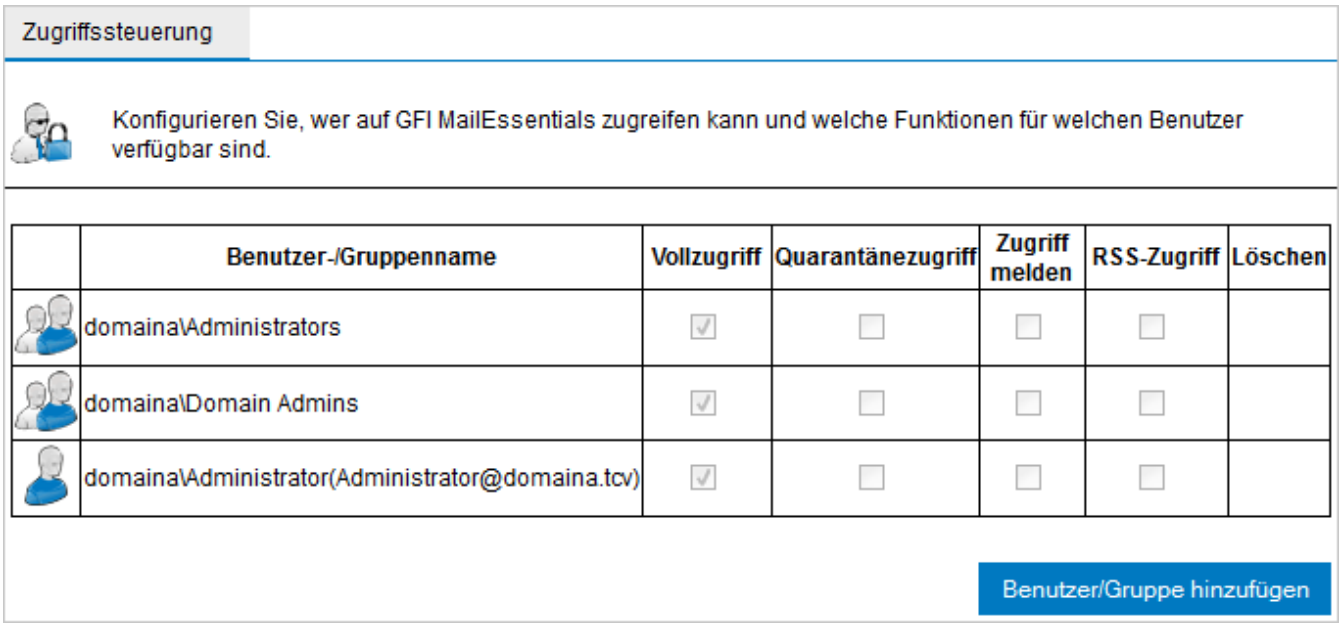
HINWEIS

Die Konfiguration der Zugriffssteuerung auf der Weboberfläche ist nur möglich, wenn GFI MailEssentials im IIS-Modus ausgeführt wird und über das Netzwerk zugänglich ist. Die Zugriffssteuerung kann nicht vom Switchboard konfiguriert werden, wenn GFI MailEssentials im lokalen Modus ausgeführt wird. Weitere Informationen finden Sie unter „Zugriffssteuerungsliste“ (Seite 256).

Die Gruppe **Domänenadministratoren** (nur in einer Active Directory-Umgebung) und das Serveradministratorkonto sowie die dazugehörige Gruppe erhalten automatisch Berechtigungen für den Vollzugriff auf alle Funktionen von GFI MailEssentials.

Andere Benutzer oder Gruppen können vollen oder partiellen Zugriff auf bestimmte Funktionen von GFI MailEssentials erhalten. So fügen Sie Benutzer zur Zugriffssteuerungsliste hinzu:

1. Wählen Sie in GFI MailEssentials Configuration die Optionen **Allgemeine Einstellungen > Zugriffssteuerung** aus. Fügen Sie Domänenbenutzer oder Gruppen hinzu, und wählen Sie die Produktfunktionen aus, auf die sie Zugriff erhalten sollen.



Screenshot 131: Einstellungen für die Zugriffskontrolle

2. Klicken Sie auf **Benutzer/Gruppe hinzufügen**.

3. Geben Sie im Dialogfeld **Benutzersuchen** den Benutzer- oder Gruppennamen ein, der hinzugefügt werden soll, und klicken Sie auf **Namen prüfen**.

4. GFI MailEssentials zeigt die Liste der gefundenen Benutzer/Gruppen an. Wählen Sie die Benutzer/Gruppen aus, die hinzugefügt werden sollen, und klicken Sie auf **Senden**.

5. Wählen Sie die Funktionen aus, auf die die neu hinzugefügten Benutzer/Gruppen Zugriff erhalten sollen.

Berechtigung	Beschreibung
Vollzugriff	Die Benutzer können auf alle Funktionen des Produkts zugreifen und diese konfigurieren.
Quarantänezugriff	Ermöglicht den Zugriff auf die Quarantänesuche und Suchordner.
Zugriff melden	Ermöglicht Benutzern, Berichte zu generieren.
RSS-Zugriff	Ermöglicht Benutzern, Quarantäne-RSS-Feeds zu abonnieren.

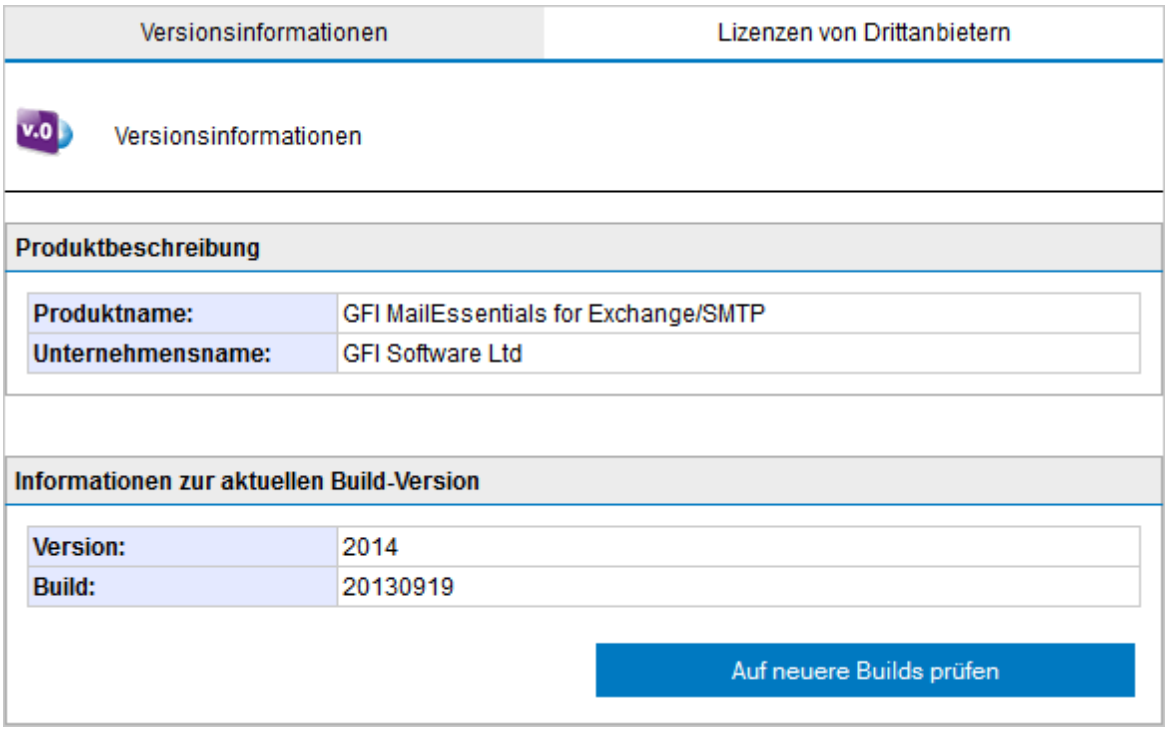
6. Klicken Sie auf **Übernehmen**.

11 Verschiedene Themen

Themen in diesem Kapitel:

11.1 Installationsinformationen 253
11.2 Namen der virtuellen Verzeichnisse 254
11.3 Benutzeroberflächenmodus 254
11.4 Fehlgeschlagene E-Mails 259
11.5 Rückverfolgung 260
11.6 POP2Exchange - E-Mails vom POP3-Server herunterladen 262
11.7 Verschieben von Spam-E-Mails in Benutzerpostfachordner 266
11.8 Verschieben von Spam in einen Exchange 2010-Ordner 268
11.9 Synchronisieren der Konfigurationsdaten 269
11.10 Deaktivieren der E-Mail-Verarbeitung 281
11.11 E-Mail-Sicherung vor und nach der Verarbeitung 282
11.12 Fernzugriffsports 283
11.13 Überwachen der Virus Scanning API 284

11.1 Installationsinformationen



Screenshot 132: Seite mit Versionsinformationen

Öffnen Sie zum Anzeigen der Versionsinformationen von GFI MailEssentials den Knoten **Info**. Die Registerkarte **Versionsinformationen** enthält die Installationsversion und die Build-Nummer von GFI MailEssentials.

Sie können überprüfen, ob Sie das neueste Build von GFI MailEssentials auf Ihrem Rechner installiert haben, indem Sie auf **Auf neuere Builds prüfen** klicken.

> **HINWEIS**
>
> Geben Sie immer Ihre GFI-Version und Build-Informationen an, wenn Sie den GFI-Support kontaktieren.

Auf der Registerkarte **Lizenzen von Drittanbietern** sind die Drittanbieterkomponenten aufgeführt, die von GFI MailEssentials verwendet werden.

11.2 Namen der virtuellen Verzeichnisse

Die Standardnamen für die virtuellen Verzeichnisse von GFI MailEssentials und Quarantäne-RSS sind **MailEssentials** und **MailEssentialsRSS**. Die Namen der virtuellen Verzeichnisse können geändert werden, dies wird jedoch nicht empfohlen.

> **HINWEIS**
>
> Wenn GFI MailEssentials so konfiguriert wird, dass ein Zugriff nur über den lokalen Rechner möglich ist, kann das virtuelle Verzeichnis GFI MailEssentials Configuration nicht konfiguriert werden.

1. Starten Sie GFI MailEssentialsSwitchboard unter **Start > Programme > GFI MailEssentials > Switchboard**.

2. Geben Sie im Bereich **Optionen für ISS-Benutzeroberflächenmodus** die gewünschten Namen für folgende virtuelle Verzeichnisse an:

» GFI MailEssentials Configuration – Geben Sie den gewünschten Namen im Feld **Virtuelles Verzeichnis** ein.

» Virtuelles Quarantäne-RSS-Verzeichnis – Geben Sie den gewünschten Namen im Feld **Virtuelles RSS-Verzeichnis** ein.

3. Klicken Sie auf **Übernehmen**.

4. Klicken Sie auf **OK**, und warten Sie, während die neuen Einstellungen übernommen werden.

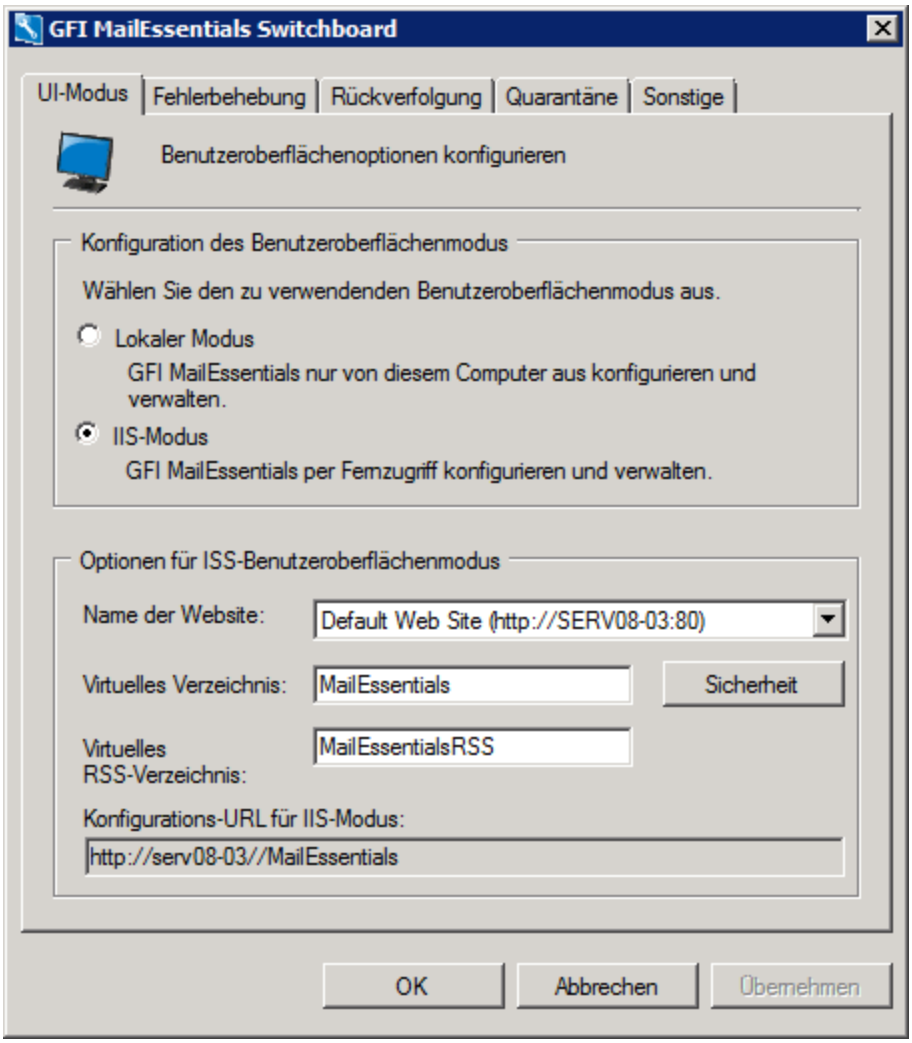
5. Wenn der Vorgang abgeschlossen ist, klicken Sie auf **OK**.

11.3 Benutzeroberflächenmodus

Die Benutzeroberfläche von GFI MailEssentials kann auf zwei Arten verwendet werden: entweder nur auf dem Installationsrechner (lokaler Modus) oder über HTTP über das Netzwerk (IIS-Modus).

So wählen Sie den Modus aus:

1. Starten Sie dasGFI MailEssentials-Switchboard unter **Start > Programme > GFI MailEssentials > Switchboard**.



Screenshot 133: GFI MailEssentials Switchboard: UI-Modus

2. Wählen Sie im Bereich **UI-Modus** die gewünschte Option aus:

Option	Beschreibung
Lokaler Modus	GFI MailEssentials wird in einem HTML-Viewer geladen, der nur auf dem Rechner zugänglich ist, auf dem GFI MailEssentials installiert ist. **HINWEIS** Im lokalen Modus: » Spam-Übersichtslinks funktionieren nicht » Das Benutzerportal steht nicht zur Verfügung. Die Benutzer können keine persönlichen Whitelists, Blocklists und Quarantäneordner verwalten. Weitere Informationen finden Sie unter „Endbenutzeraktionen“ (Seite 19).
IIS-Modus (empfohlen)	GFI MailEssentials wird in Ihrem Standard-Webbrowser mit den IIS-Einstellungen geladen, die bei der Installation konfiguriert wurden. Die Benutzeroberfläche ist auch über das Netzwerk über HTTP zugänglich. **HINWEIS** Die IIS-Einstellungen können mittels Website-Name, virtuellem Verzeichnis und Feldern des virtuellen RSS-Verzeichnisses geändert werden. Die Optionen zur **Sicherheit** aktivieren die Konfiguration einer Zugriffssteuerungsliste und der IIS-Authentifizierung.

HINWEIS

Einige Dienste werden vorübergehend angehalten, während dieser Vorgang ausgeführt wird. Dies kann den E-Mail-Fluss und/oder die E-Mail-Scans beeinträchtigen.

3. Klicken Sie auf **Ja**, um die angezeigten Dienste neu zu starten.

4. Klicken Sie auf **OK**.

11.3.1 IIS-Sicherheitseinstellungen

Mithilfe der Schaltfläche **Sicherheit** auf der Registerkarte „UI-Modus“ können Sie eine Zugriffssteuerungsliste und die Authentifizierungsmethode konfigurieren.

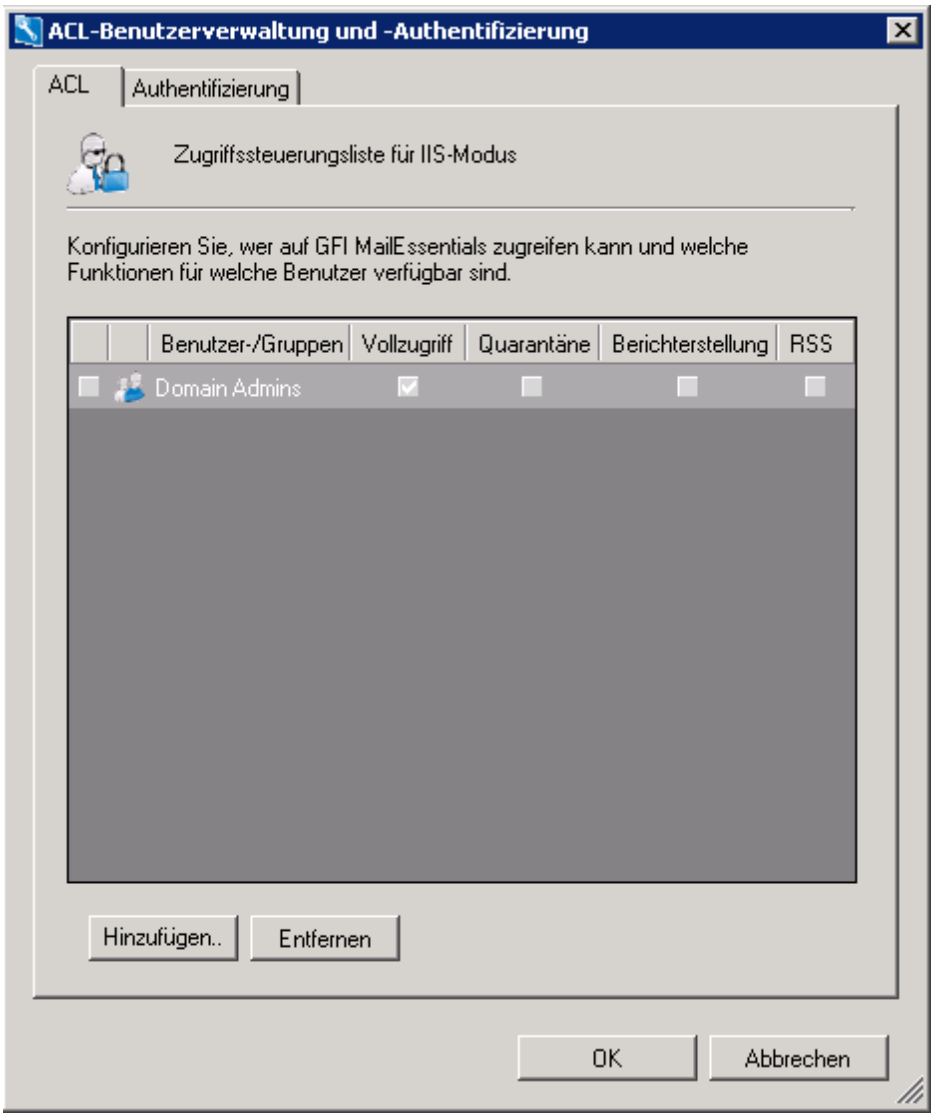
Zugriffssteuerungsliste

In der Zugriffssteuerungsliste wird angegeben, wer Zugriff auf GFI MailEssentials hat und welche Funktionen für welche Benutzer und Gruppen verfügbar sind. Administratoren haben standardmäßig vollständigen Zugriff auf GFI MailEssentials; Sie können jedoch bestimmte Benutzer und Gruppen mit unterschiedlichen Zugriffstypen angeben.

So fügen Sie einen Benutzer hinzu:

1. Öffnen Sie das Switchboard durch Klicken auf **Start > Programme > GFI MailEssentials > Switchboard**.

2. Wählen Sie die Registerkarte **UI-Modus** aus. Klicken Sie auf **IIS-Modus**, und wählen Sie die die Option **Sicherheit**.



Screenshot 134: IIS-Sicherheit - Registerkarte „ACL“

3. Klicken Sie auf **Hinzufügen**, und geben Sie den Namen des Benutzers oder der Gruppe an, der/die zur Liste hinzugefügt werden soll.

4. Wählen Sie den zu gewährenden Zugriff aus. Folgende Optionen sind verfügbar:

Berechtigung	Beschreibung
Vollzugriff	Die Benutzer können auf alle Funktionen des Produkts zugreifen und diese konfigurieren.
Quarantänezugriff	Ermöglicht den Zugriff auf die Quarantänesuche und Suchordner.
Zugriff melden	Ermöglicht Benutzern, Berichte zu generieren.
RSS-Zugriff	Ermöglicht Benutzern, Quarantäne-RSS-Feeds zu abonnieren.

5. Klicken Sie auf **OK**, um die Einrichtung abzuschließen.

Wählen Sie dem Entfernen einer Zugriffsberechtigung einen Benutzer oder eine Gruppe aus, und klicken Sie auf **Entfernen**.

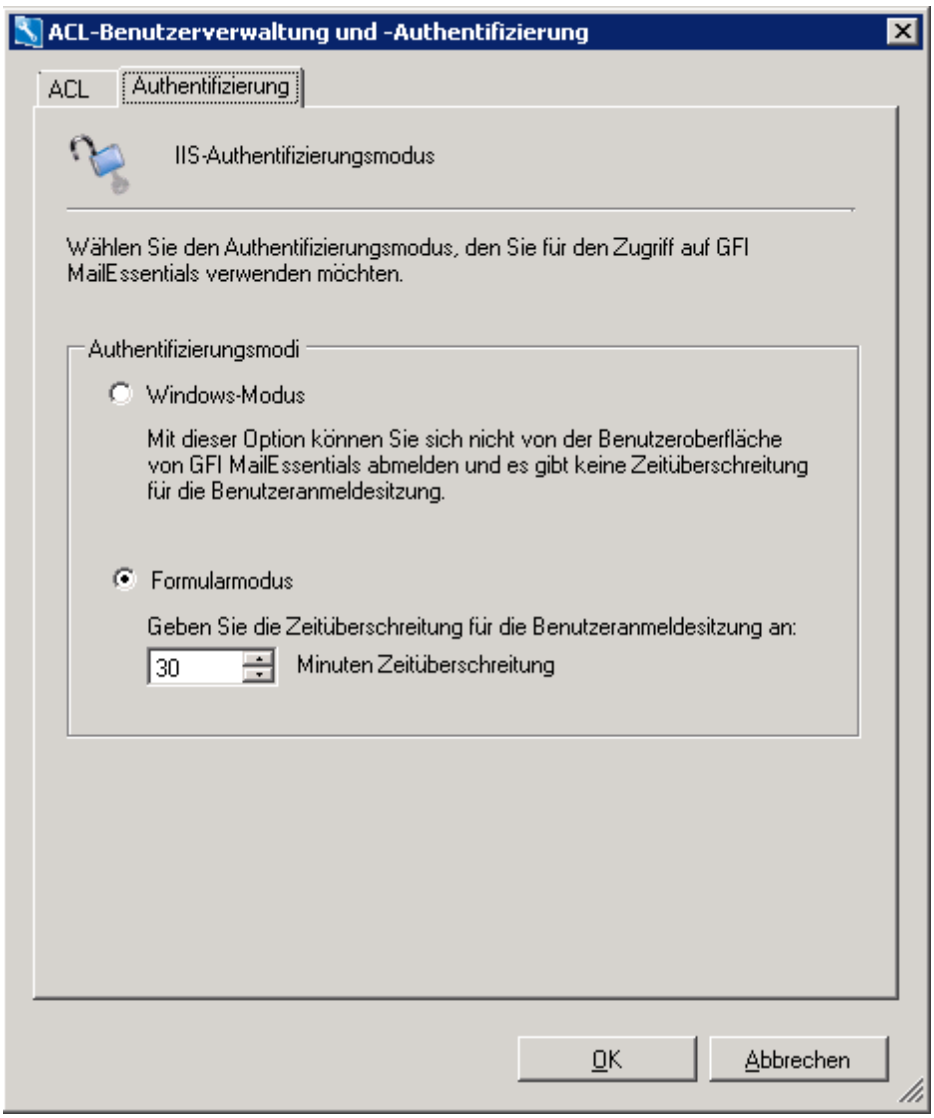
IIS-Authentifizierungsmodus

Im IIS-Authentifizierungsmodus können Sie die Authentifizierungsmethode auswählen, die beim Zugriff auf GFI MailEssentials angewendet werden soll.

1. Öffnen Sie das Switchboard durch Klicken auf **Start > Programme > GFI MailEssentials > Switchboard**.

2. Wählen Sie die Registerkarte **UI-Modus** aus. Klicken Sie auf **IIS-Modus**, und wählen Sie die die Option **Sicherheit**.

3. Wählen Sie die Registerkarte **Authentifizierung** aus.


ACL-Benutzerverwaltung und -Authentifizierung
ACL
Authentifizierung
IIS-Authentifizierungsmodus
Wählen Sie den Authentifizierungsmodus, den Sie für den Zugriff auf GFI MailEssentials verwenden möchten.
Authentifizierungsmodi
Windows-Modus
Mit dieser Option können Sie sich nicht von der Benutzeroberfläche von GFI MailEssentials abmelden und es gibt keine Zeitüberschreitung für die Benutzeranmeldesitzung.
Formularmodus
Geben Sie die Zeitüberschreitung für die Benutzeranmeldesitzung an:
30
Minuten Zeitüberschreitung
OK
Abbrechen

Screenshot 135: IIS-Sicherheit - Registerkarte „Authentifizierung“

4. Wählen Sie eine der verfügbaren Optionen aus:

Option	Beschreibung
Windows-Modus	Mithilfe der Windows-Authentifizierung verwendet GFI MailEssentials die Anmeldeinformationen des aktuell angemeldeten Benutzers und bietet keine Abmeldefunktion und keine automatische Zeitüberschreitung der Benutzeroberflächensitzung.
Formularmodus	(Standard) Bei der Formularauthentifizierung können sich Benutzer abmelden. Außerdem können Sie eine automatische Zeitüberschreitung der Benutzeroberflächensitzung konfigurieren. Dies wird empfohlen, wenn Endbenutzer auf ihre GFI MailEssentials-Benutzerkonsole zugreifen, besonders wenn dies von öffentlichen Computern geschieht.

5. Klicken Sie auf **OK**, um die Einstellung zu speichern.

11.4 Fehlgeschlagene E-Mails

Es kann vorkommen, dass die E-Mail-Sicherheitskomponenten oder Inhaltsfilter von GFI MailEssentials eine E-Mail nicht scannen können, da diese beispielsweise beschädigte Header-Informationen enthält. In diesem Fall blockiert GFI MailEssentials die E-Mail, da sie schädliche Inhalte aufweisen könnte, und verschiebt sie in den folgenden Ordner:

<GFI MailEssentials Installationspfad>\EmailSecurity\failedmails

11.4.1 Erneute Verarbeitung erwünschter fehlgeschlagener E-Mails

Es wird empfohlen, den Support von GFI zu kontaktieren, nachdem mehrere E-Mails in den Ordner **failedmails** verschoben wurden. Sobald das Problem behoben wurde, können die E-Mails erneut mit GFI MailEssentials gescannt werden, um festzustellen, ob sie sicher sind und zugestellt werden können.

> **HINWEIS**
>
> Dateien mit der Endung PROP im Ordner **failedmails** werden zu Fehlerbehebungszwecken verwendet. Sie können bei der erneuten Verarbeitung der E-Mails gelöscht werden.

GFI MailEssentials ist auf Microsoft® Exchange Server 2007/2010 installiert

1. Ändern Sie im Ordner **failedmails** die Erweiterung der TXT-Dateien zu EML.

> **HINWEIS**
>
> Um automatisch alle TXT-Dateien im Ordner **failedmails** in EML-Dateien umzubenennen, wechseln Sie in der Eingabeaufforderung zum Ordner **failedmails**, und führen Sie folgenden Befehl aus:
>
> `ren *.txt *.eml`

2. Verschieben Sie die umbenannten Dateien in den folgenden Ordner:

<Laufwerk>\Programme\Microsoft\Exchange Server\TransportRoles\Replay

GFI MailEssentials ist auf Microsoft® Exchange Server 2003 installiert

Verschieben Sie die E-Mails (TXT-Format) aus dem Ordner **failedmails** in den folgenden Ordner:

<Installationspfad>\Exchsrvr\Mailroot\vsi 1\PickUp

GFI MailEssentials ist auf dem Gateway-Server installiert

Verschieben Sie die E-Mails (TXT-Format) aus dem Ordner **failedmails** in den folgenden Ordner:

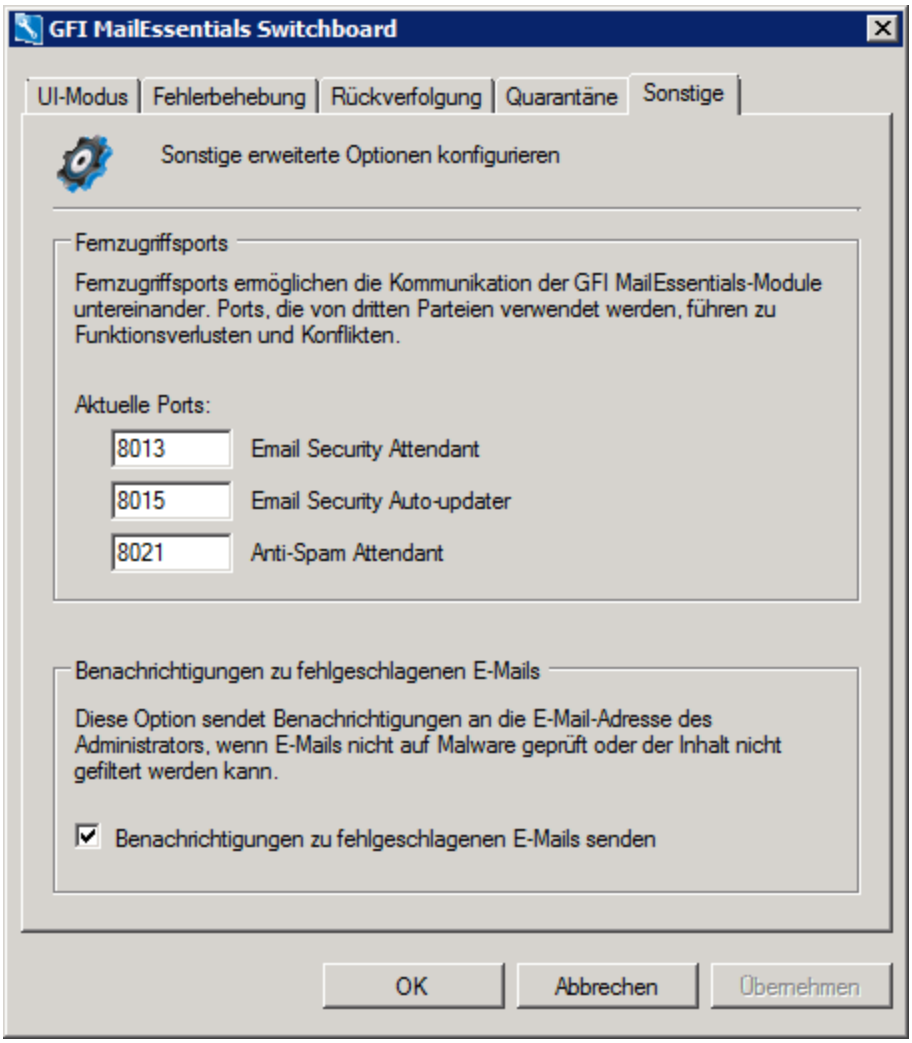
<Laufwerk>\Inetpub\mailroot\Pickup

11.4.2 Benachrichtigungen über fehlgeschlagene E-Mails

GFI MailEssentials kann so konfiguriert werden, dass der Administrator über fehlgeschlagene E-Mail-Verarbeitungen benachrichtigt wird.

Konfigurieren Sie die Administrator-E-Mail-Adresse in den allgemeinen Einstellungen von GFI MailEssentials. Weitere Informationen finden Sie unter „Administrator-E-Mail-Adresse“ (Seite 245).

1. Starten Sie das GFI MailEssentials Switchboard über **Start > Programme > GFI MailEssentials > Switchboard**, und wählen Sie die Registerkarte **Weitere** aus.



Screenshot 136: Benachrichtigungen über fehlgeschlagenen E-Mails aktivieren

2. Wählen Sie **Benachrichtigungen zu fehlgeschlagenen E-Mails senden** aus.

3. Klicken Sie auf **Übernehmen**.

> **HINWEIS**
>
> Einige Dienste werden vorübergehend angehalten, während dieser Vorgang ausgeführt wird. Dies kann den E-Mail-Fluss und/oder die E-Mail-Scans beeinträchtigen.

4. Klicken Sie auf **Ja**, um die angezeigten Dienste neu zu starten.

5. Klicken Sie auf **OK**.

11.5 Rückverfolgung

GFI MailEssentials bietet die Möglichkeit, Protokolldateien für Debugging-Zwecke zu erstellen. Verwenden Sie die Rückverfolgung für Fehlerbehebungszwecke oder bei Kontaktaufnahme mit dem Support von GFI. Deaktivieren Sie die Rückverfolgung, falls Leistungsprobleme auf dem GFI MailEssentials-Rechner auftreten.

Wenn diese Funktion aktiviert ist, speichert GFI MailEssentials verschiedene Protokolldateien in den folgenden Ordnern:

» <*GFI MailEssentials Installationspfad*>*GFI**MailEssentials*\DebugLogs\

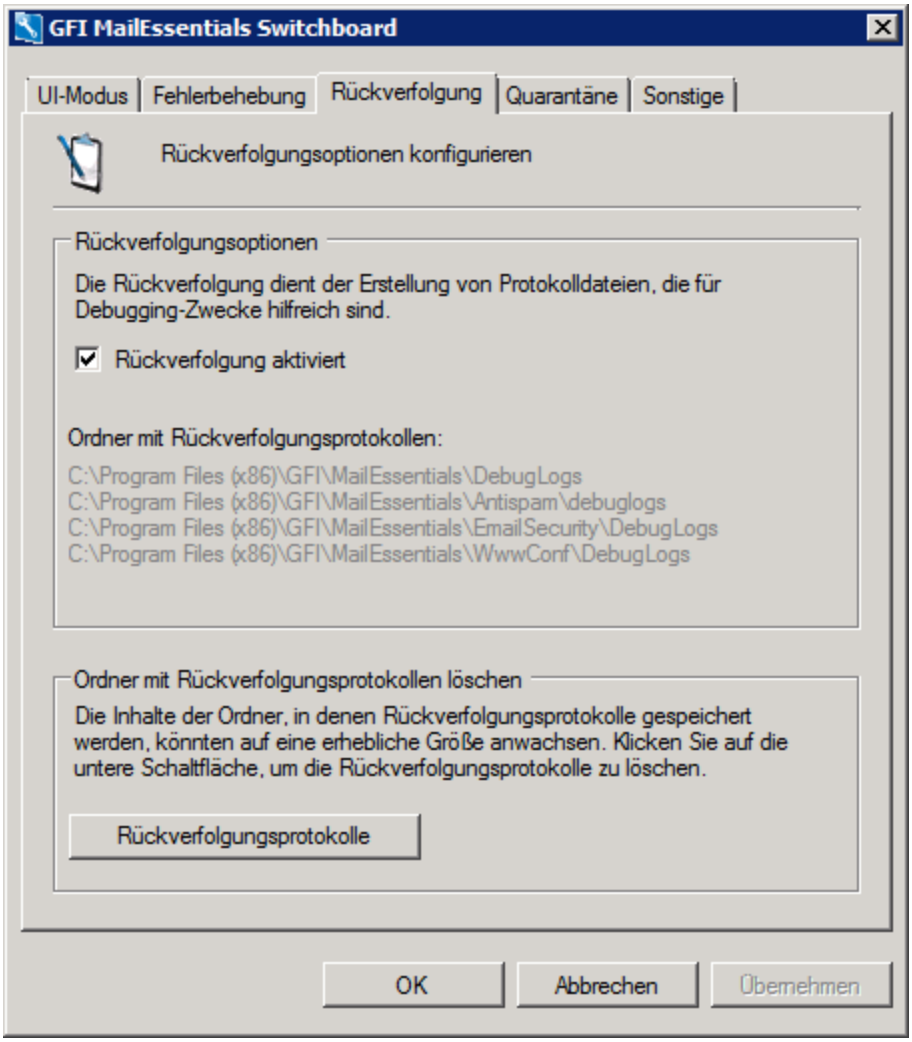
» <*GFI MailEssentials Installationspfad*>*GFI**MailEssentials*\DebugLogs\

» <*GFI MailEssentials Installationspfad*>*GFI**MailEssentials*\AntiSpam\DebugLogs\

» <*GFI MailEssentials Installationspfad*>*GFI**MailEssentials*\WwwConf\DebugLogs\

So aktivieren oder deaktivieren Sie die Rückverfolgung:

1. Starten Sie das GFI MailEssentials Switchboard über **Start > Programme > GFI MailEssentials > Switchboard**, und wählen Sie die Registerkarte **Rückverfolgung** aus.



Screenshot 137: Rückverfolgungsoptionen konfigurieren

2. Aktivieren oder deaktivieren Sie die Option **Rückverfolgung aktiviert**.

> **HINWEIS**
>
> Einige Dienste werden vorübergehend angehalten, während dieser Vorgang ausgeführt wird. Dies kann den E-Mail-Fluss und/oder die E-Mail-Scans beeinträchtigen.

3. Klicken Sie auf **Ja**, um die angezeigten Dienste neu zu starten.

4. Klicken Sie auf **OK**.

Rückverfolgungsprotokolle löschen

So löschen Sie alle Rückverfolgungsprotokolle:

1. Starten Sie das GFI MailEssentials Switchboard über **Start > Programme > GFI MailEssentials > Switchboard**, und wählen Sie die Registerkarte **Rückverfolgung** aus.

> **HINWEIS**
>
> Einige Dienste werden vorübergehend angehalten, während dieser Vorgang ausgeführt wird. Dies kann den E-Mail-Fluss und/oder die E-Mail-Scans beeinträchtigen.

2. Klicken Sie auf **Rückverfolgungsprotokolle löschen** und anschließend auf **Ja**, um die angezeigten Services neu zu starten.

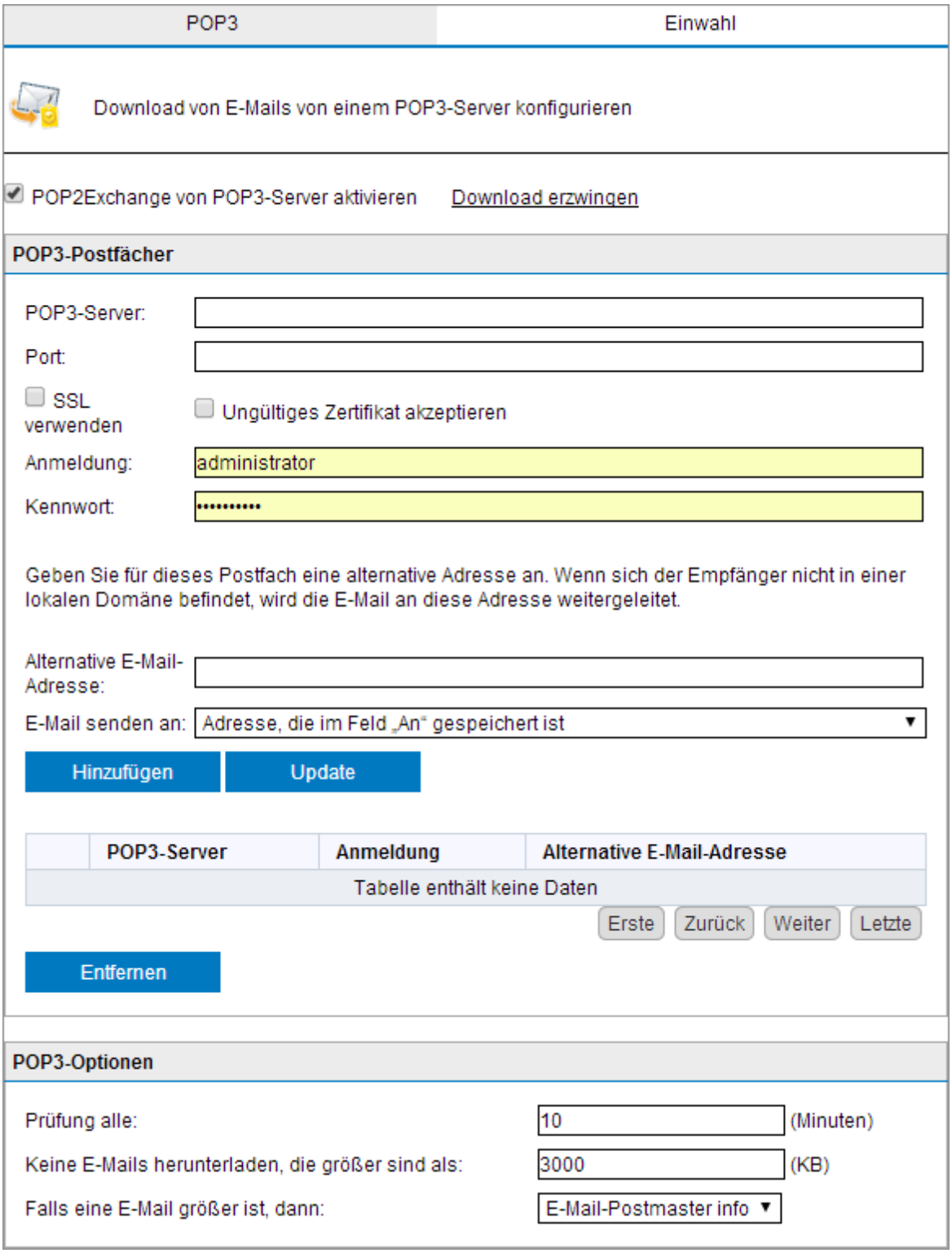
3. Klicken Sie zum Abschluss auf **OK**.

11.6 POP2Exchange – E-Mails vom POP3-Server herunterladen

POP2Exchange lädt E-Mails von einem POP3-Server herunter, verarbeitet sie und sendet sie an den lokalen Mailserver. Für GFI MailEssentials wird empfohlen, die Verwendung von POP3 nach Möglichkeit zu vermeiden und stattdessen SMTP zu verwenden, da POP3 für E-Mail-Clients konzipiert ist, nicht für Mailserver. Es ist jedoch trotzdem möglich, POP3 mit GFI MailEssentials zum Abrufen von E-Mails zu verwenden. Dies kann erforderlich sein, wenn keine statische IP-Adresse für SMTP verfügbar ist.

11.6.1 Konfigurieren des POP3-Downloaders

1. Öffnen Sie den Knoten **POP2Exchange**.



Screenshot 138: Der GFI MailEssentials POP3-Downloader

2. Wählen Sie auf der Registerkarte **POP3** die Option **POP2Exchange vom POP3-Server aktivieren**, um den POP3-Downloader zu aktivieren.

3. Geben Sie in das Feld **POP3-Postfächer** die Informationen zum POP3-Server ein, von dem E-Mails heruntergeladen werden:

Option	Beschreibung
POP3-Server	Geben Sie die IP-Adresse des POP3-Servers ein, von dem E-Mails heruntergeladen werden.
Port	Geben Sie den POP3-Port an. Standardmäßig wird für POP3 der Port 110 oder 995 verwendet, wenn eine sichere Verbindung genutzt wird.
SSL verwenden	Wählen Sie, ob der POP3-Server eine sichere Verbindung erfordert.
Ungültiges Zertifikat akzeptieren	Wählen Sie diese Option, wenn Sie ungültige Zertifikate vom POP3-Server ignorieren möchten. Es wird empfohlen, diese Option zu deaktivieren und sicherzustellen, dass alle Zertifikate gültig sind.
Anmeldung und Kennwort	Geben Sie die Anmeldeinformationen zu Anmeldung am POP3-Postfach an.
Alternative E-Mail-Adresse	Wenn die E-Mails im Postfach an einen Empfänger gerichtet sind, der sich nicht in einer der lokalen GFI MailEssentials-Domänen befindet, werden E-Mails an diese Adresse weitergeleitet. Stellen Sie sicher, dass dies eine lokale Adresse ist, die auf dem E-Mail-Server konfiguriert ist und von GFI MailEssentials geschützt wird.
E-Mail senden an:	Auswählen: » **Adresse, die im Feld „An“ gespeichert ist**: GFI MailEssentials analysiert den E-Mail-Header und leitet die E-Mail entsprechend weiter. Falls die E-Mail-Analyse fehlschlägt, wird die E-Mail an die Adresse gesendet, die als **Alternative E-Mail-Adresse** angegeben wurde. » **Alternative E-Mail-Adresse**: GFI MailEssentials analysiert nicht die E-Mail-Header, und alle E-Mails von diesem Postfach werden an die Adresse weitergeleitet, die in **Alternative E-Mail-Adresse** angegeben wurde.

4. Klicken Sie auf **Add**, um die POP3-Serverdetails hinzuzufügen. Wählen Sie einen hinzugefügten POP3-Server aus, und klicken Sie auf **Aktualisieren**, um ihn durch die neu eingegebenen Einstellungen zu ersetzen.

5. Wiederholen Sie die obigen Schritte, um mehrere POP3-Server hinzuzufügen.

6. Konfigurieren Sie unter **POP3-Optionen** Folgendes:

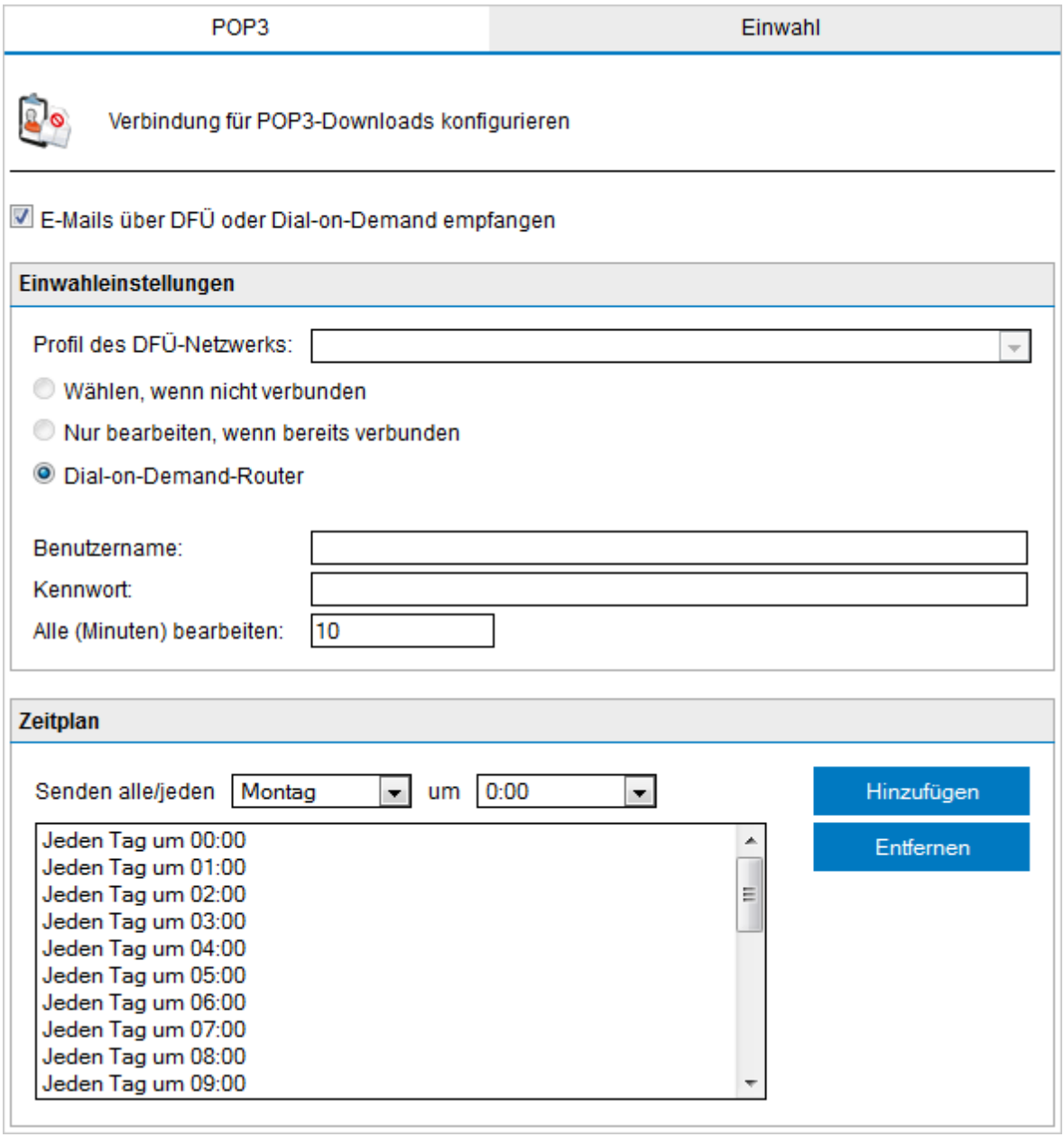
Option	Beschreibung
Alle (Minuten) prüfen	Geben Sie das Download-Intervall in Minuten an.
Keine E-Mails herunterladen, die größer sind als:	Geben Sie die die maximale Download-Größe in KB an. E-Mails, die größer sind als der angegebene Wert, werden nicht heruntergeladen.
Falls eine E-Mail größer ist, dann:	Sie können wählen, ob E-Mails, die größer sind als erlaubt, zu löschen sind, oder ob eine Benachrichtigung an den Postmaster geschickt werden soll.

8. Klicken Sie auf **Übernehmen**.

11.6.2 Konfigurieren von Optionen für eine DFÜ-Verbindung (Dial-Up)

1. Öffnen Sie den Knoten **POP2Exchange**, und wählen Sie die Registerkarte **Einwahl**.

2. Wählen Sie **E-Mails über Einwahl oder Dial-on-Demand empfangen**.



Screenshot 139: Einwahloptionen

3. Wählen Sie ein DFÜ-Netzwerk-Profil aus, und konfigurieren Sie einen Anmeldenamen und ein Kennwort. Die folgenden Optionen sind verfügbar:

Option	Beschreibung
Dieses DFÜ-Netzwerkprofil verwenden	Wählen Sie das gewünschte DFÜ-Netzwerk-Profil aus.
Wählen, wenn nicht verbunden	GFI MailEssentials wählt nur ein, wenn keine Verbindung besteht.
Nur bearbeiten, wenn bereits verbunden	GFI MailEssentials verarbeitet eine E-Mail nur, wenn bereits eine Verbindung besteht.
Dial-on-Demand-Router:	Wenn Sie eine Internetverbindung nutzen, die automatisch hergestellt wird (z. B. über einen Dial-on-Demand-Router), wählen Sie diese Option aus. GFI MailEssentials empfängt E-Mails im angegebenen Intervall, ohne dabei eine DFÜ-Einwahl auszulösen.

Option	Beschreibung
Benutzername und Kennwort	Geben Sie die Informationen zur Anmeldung bei Ihrem ISP an.
Alle (Minuten) bearbeiten	Geben Sie das Intervall in Minuten ein.

4. Geben Sie im Bereich **Zeitplan** die Stunden an, zu denen sich GFI MailEssentials einwählen soll, um E-Mails abzurufen.

5. Klicken Sie auf **Übernehmen**.

11.7 Verschieben von Spam-E-Mails in Benutzerpostfachordner

Wenn GFI MailEssentials auf einem Microsoft® Exchange-Server installiert ist, können Spam-E-Mails in einem Benutzerpostfachordner gespeichert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

Ist GFI MailEssentials **NICHT** auf einem Microsoft® Exchange-Server installiert, können Spam-E-Mails nicht mithilfe der Spam-Aktionen in den Postfachordner eines bestimmten Benutzers weitergeleitet werden. Die E-Mails können aber auf folgende Weise in das Postfach des Benutzers geleitet werden.

11.7.1 Microsoft® Exchange Server 2003

GFI MailEssentials beinhaltet das Regel-Manager-Dienstprogramm, das E-Mails, die als Spam gekennzeichnet sind, automatisch in das Postfach des Benutzers verschiebt.

> **WICHTIG**
>
> Um den Regel-Manager zu verwenden, wählen Sie in den Spam-Aktionen die Option **Die E-Mail mit einem bestimmten Text kennzeichnen** aus, und legen Sie eine Kennzeichnung fest.

Regel-Manager auf dem Microsoft® Exchange-Server installieren

1. Navigieren Sie auf dem GFI MailEssentials-Rechner zu:

<GFI MailEssentials Installationspfad>\GFI\MailEssentials\Antispam\

2. Kopieren Sie die folgenden Dateien in einen Ordner auf dem Microsoft® Exchange-Server:

- rulemgmtres.dll
- rulemgmt.exe
- rule.dll
- gfi_log.dll

3. Öffnen Sie auf dem Microsoft® Exchange-Server die Eingabeaufforderung, und wechseln Sie in das Verzeichnis, in das die Regel-Manager-Dateien kopiert wurden.

4. Geben Sie in der Eingabeaufforderung Folgendes ein: `regsvr32 rule.dll`

5. Klicken Sie zur Bestätigung auf **OK**.

Regel-Manager starten

1. Navigieren Sie auf dem Microsoft® Exchange-Server zu dem Verzeichnis, in das die Regel-Manager-Dateien kopiert wurden, und öffnen Sie **rulemgmt.exe**.

2. Wählen Sie ein Microsoft® Outlook-Profil (MAPI-Profil) aus, oder erstellen Sie ein neues Profil für die Anmeldung (nur bei erstmaliger Verwendung des Regel-Managers).

3. Klicken Sie auf **OK**, um den Regel-Manager zu starten.

4. Im Hauptfenster des Regel-Managers werden alle Postfächer angezeigt, die auf dem Microsoft® Exchange-Server aktiviert sind. Die Farbe der Postfächer gibt den jeweiligen Status an:

» Blau – Für das Postfach sind Regeln konfiguriert.

» Schwarz – Für das Postfach sind keine Regeln konfiguriert.

Erstellen neuer Regeln

1. Wählen Sie die Postfächer aus, für die eine Regel festgelegt werden soll, und klicken Sie auf **Konfigurieren...**.

> **HINWEISE**
>
> 1. Neue Regeln können auch für Postfächer hinzugefügt werden, die bereits Regeln enthalten.
> 2. Sie können mehrere Postfächer auswählen, für die dieselbe Regel gelten soll.

2. Geben Sie im Textfeld **Regelbedingung** die Kennzeichnung ein, die Sie in den Spam-Aktionen von GFI MailEssentials für Spam-E-Mails definiert haben.

3. Legen Sie die **Regelaktion** fest:

» Wählen Sie **Löschen** aus, um E-Mails zu löschen, deren Betreff die Regelbedingung enthält.

» Wählen Sie **Verschieben nach:** aus, um Spam-E-Mails in einen Ordner im Postfach zu verschieben. Geben Sie den Pfad des Ordners ein, in dem Spam-E-Mails gespeichert werden sollen. Wenn Sie 'Posteingang\Spam' angeben, wird ein Spam-Ordner im Posteingangsordner erstellt. Wenn Sie nur 'Spam' angeben, wird der Ordner auf der obersten Ebene erstellt (auf derselben Ebene wie der Posteingang).

4. Klicken Sie auf **Übernehmen**, um die erstellten Regeln zu speichern.

Verwalten mehrerer Regeln

Sie können mehrere Regeln für ein Postfach erstellen.

Beispiel: E-Mails mit der Kennzeichnung `[Phishing]` sollen gelöscht und E-Mails mit der Kennzeichnung `[SPAM]` in den Spam-Ordner im Posteingang verschoben werden.

1. Doppelklicken Sie auf ein Postfach, um das Dialogfeld für Regeln zu öffnen.

2. Die Liste der Regeln, die für das ausgewählte Postfach gelten, wird angezeigt.

» Klicken Sie auf **Regel hinzufügen**, um eine neue Regel hinzuzufügen.

» Wählen Sie eine Regel aus, und klicken Sie auf **Regel bearbeiten**, um die Einstellungen der ausgewählten Regel zu ändern.

» Wählen Sie eine Regel aus, und klicken Sie auf **Regel löschen**, um die ausgewählte Regel zu löschen.

3. Klicken Sie auf **Übernehmen**, um die Einstellungen zu speichern.

11.7.2 Microsoft® Exchange 2007/2010

Um Microsoft® Exchange 2007/2010 so zu konfigurieren, dass gekennzeichnete E-Mails in den Junk-Ordner des Benutzerpostfachs weitergeleitet werden, muss eine Transportregel erstellt werden.

WICHTIG

Wählen Sie in den Spam-Aktionen von GFI MailEssentials nur die Option 'Die E-Mail mit einem bestimmten Text kennzeichnen' aus. Bei allen anderen Aktionen werden Spam-Nachrichten bereits abgefangen, bevor sie in das Postfach des Benutzers gelangen, und die konfigurierten Transportregeln kommen nicht zur Anwendung.

So erstellen Sie in Exchange 2007/2010 eine Transportregel:

1. Starten Sie die Microsoft® Exchange-Verwaltungskonsole.

2. Navigieren Sie zu **Microsoft Exchange > Organisationskonfiguration > Hub-Transport**, und wählen Sie den Knoten **Transportregeln** aus.

3. Klicken Sie auf **Neue Transportregel**.

4. Geben Sie einen Namen für die neue Regel ein (z. B. GFI MailEssentials `SPAM`), und klicken Sie auf **Weiter**.

5. Wählen Sie im Bereich **Bedingungen** die Option **Wenn Betreff bestimmte Wörter enthält** aus.

6. Klicken Sie im Bereich **Regel bearbeiten** auf **Bestimmte Wörter**, um die Wörter einzugeben, die als Kennzeichnung verwendet werden sollen. Geben Sie die Kennzeichnung ein, die in den Spam-Aktionen des jeweiligen Spam-Filters angegeben wurden (z. B. `[SPAM]`), und klicken Sie auf **Hinzufügen**. Klicken Sie auf **OK**, wenn Sie alle Wörter hinzugefügt haben, und klicken Sie dann auf **Weiter**.

7. Wählen Sie im Bereich **Aktionen** die Option **Spam Confidence Level auf Wert festlegen** aus.

8. Klicken Sie im Bereich **Regel bearbeiten** auf **0**, und legen Sie das Confidence Level auf **9** fest. Klicken Sie auf **OK** und dann auf **Weiter**.

9. Definieren Sie bei Bedarf Ausnahmen für diese Transportregel, und klicken Sie auf **Weiter**.

10. Klicken Sie auf **Neu**, um die neue Transportregel zu erstellen.

HINWEIS

Stellen Sie sicher, dass der Junk-Mail-Ordner in den Benutzerpostfächern aktiviert ist.

Die erstellte Transportregel leitet nun alle E-Mails mit der angegebenen GFI MailEssentials-Kennzeichnung in den Junk-Mail-Ordner der Benutzer weiter.

11.8 Verschieben von Spam in einen Exchange 2010-Ordner

Wenn GFI MailEssentials auf einem Microsoft® Exchange 2010-Server installiert ist, muss für die Anti-Spam-Aktion **E-Mail an folgendes Postfach zustellen - Im Unterordner des Exchange-Postfachs** ein dedizierter Benutzer erstellt werden. Konfigurieren Sie den dedizierten Benutzer über das GFI MailEssentials Switchboard.

HINWEIS

Wird kein Benutzer konfiguriert, können Spam-Nachrichten nicht in einen Postfach-Unterordner verschoben werden.

So konfigurieren Sie einen dedizierten Benutzer:

1. Starten Sie das GFI MailEssentialsSwitchboard über **Start > Programme > GFI MailEssentials > Switchboard**.

2. Wählen Sie die Registerkarte **In Exchange verschieben** aus.

> **HINWEIS**
>
> Diese Registerkarte wird nur angezeigt, wenn GFI MailEssentials auf einem Microsoft® Exchange 2010-Server installiert ist.

3. Klicken Sie auf **Benutzerkonto angeben...**, um den dedizierten Benutzer anzugeben.

4. Wählen Sie eine der folgenden Optionen aus:

Option	Beschreibung
Spam mit einem automatisch erstellten Benutzer verschieben.	GFI MailEssentials erstellt automatisch einen Benutzer mit allen erforderlichen Rechten.
Spam mit folgendem Benutzerkonto verschieben	Ein manuell erstellter Benutzer wird verwendet. Legen Sie die Anmeldeinformationen (**Domäne\Benutzername** und **Kennwort**) eines dedizierten Benutzers fest, und klicken Sie auf **Zugriffsrechte einstellen**, um dem Benutzer die erforderlichen Rechte zuzuweisen.

> **HINWEIS**
>
> Die manuell angegebenen Benutzerinformationen dürfen nur für diese Funktion verwendet werden. Benutzername, Kennwort und sonstige Eigenschaften dürfen in Microsoft® Exchange oder Active Directory nicht geändert werden. Andernfalls funktioniert die Funktion nicht.

5. Klicken Sie auf **Fertig stellen**, um die Einstellungen zu übernehmen.

6. Klicken Sie auf **OK**.

11.9 Synchronisieren der Konfigurationsdaten

Wenn GFI MailEssentials auf mehreren Servern installiert ist, müssen die Konfigurationsdaten zwischen den Servern synchronisiert werden.

GFI MailEssentials ermöglicht dies über zwei Funktionen, die für eine regelmäßige Synchronisierung mehrerer GFI MailEssentials-Installationen sorgen:

» Anti-Spam-Synchronisationsagent – Dieser Dienst automatisiert die regelmäßige Synchronisierung der Einstellungen zwischen separaten Installationen mithilfe des Microsoft® BITS-Diensts.

» Export-/Import-Tool für Konfigurationseinstellungen – Diese Anwendung ermöglicht den manuellen Export von GFI MailEssentials-Konfigurationseinstellungen und den Import in andere Installationen.

11.9.1 Anti-Spam-Synchronisationsagent

Funktionsweise

Der Anti-Spam-Synchronisationsagent arbeitet wie folgt:

1. Ein Server, der GFI MailEssentials hostet, wird als Master-Server konfiguriert.

2. Alle anderen Server, auf denen GFI MailEssentials installiert ist, werden als Slave-Server eingerichtet.

3. Von den Slave-Servern wird über den Microsoft® BITS-Dienst eine Archivdatei mit Einstellungen in ein virtuelles IIS-Verzeichnis auf dem Master-Server hochgeladen.

4. Hat der Master-Server alle Daten der Slave-Server gesammelt, werden die Daten aus den einzelnen Archiven extrahiert und in einer zentralen Archivdatei zusammengeführt.

5. Die Slave-Server laden diese zentrale Archivdatei herunter, extrahieren sie und aktualisieren die lokale GFI MailEssentials-Installation mit den neuen Einstellungen.

> **HINWEIS**
>
> Auf allen Servern, deren Einstellungen synchronisiert werden sollen, muss dieselbe Version von GFI MailEssentials installiert sein.

> **HINWEIS**
>
> Die vom Synchronisationsagenten hoch- und heruntergeladenen Dateien sind komprimiert, um den Datenverkehr im Netzwerk zu minimieren.

Schritt 1: Konfigurieren des virtuellen Verzeichnisses für den Synchronisationsagenten auf dem Master-Server

Wichtige Hinweise

1. Es kann immer nur ein Server als Master-Server konfiguriert werden.

2. Der Master-Server muss eine der folgenden Spezifikationen erfüllen:

» Microsoft® Windows Server 2008 mit SP1 oder höher und IIS 7.0 mit BITS-Servererweiterungen sind installiert. Siehe http://go.gfi.com/?pageid=ME_InstallBITS2003

» Microsoft® Windows Server 2003 mit SP1 oder höher und IIS 6.0 mit BITS-Servererweiterung sind installiert. Siehe http://go.gfi.com/?pageid=ME_InstallBITS2008

3. Ein virtuelles IIS-Verzeichnis sollte nur auf dem Master-Server erstellt werden.

Konfiguration des virtuellen Verzeichnisses

Konfigurieren Sie in Internet Information Services (IIS) Manager wie nachfolgend beschrieben ein gemeinsames virtuelles Verzeichnis auf der Standardwebsite des Master-Servers.

IIS 7.0

a. Laden Sie die **Internet Information Services (IIS) Manager**-Konsole, klicken Sie mit der rechten Maustaste auf die Standardwebsite, und wählen Sie **Virtuelles Verzeichnis hinzufügen** aus.

b. Geben Sie im Dialogfeld **Virtuelles Verzeichnis hinzufügen** den Alias `MESynchAgent` für das virtuelle Verzeichnis ein.

c. Legen Sie einen Pfad fest, wo die Inhalte dieses virtuellen Verzeichnisses gespeichert werden sollen, und klicken Sie auf **OK**, um das virtuelle Verzeichnis hinzuzufügen.

> **HINWEIS**
>
> Merken Sie sich den konfigurierten Pfad für eine spätere Verwendung.

d. Wählen Sie das virtuelle Verzeichnis **MESynchAgent** aus, und doppelklicken Sie in der Funktionsansicht auf **SSL-Einstellungen**.

e. Deaktivieren Sie das Kontrollkästchen **SSL erfordern**, und klicken Sie auf **Übernehmen**.

f. Kehren Sie zur Funktionsansicht des neu hinzugefügten virtuellen Verzeichnisses zurück, und doppelklicken Sie auf **Authentifizierung**.

g. Stellen Sie sicher, dass nur **Standardauthentifizierung** aktiviert ist. Alle andere Optionen müssen deaktiviert sein.

h. Klicken Sie mit der rechten Maustaste auf **Standardauthentifizierung**. Klicken Sie anschließend auf **Bearbeiten…**, um die **Standarddomäne** und den **Bereich** für den Benutzernamen und das Kennwort festzulegen, die von den Slave-Rechnern für die Authentifizierung verwendet werden sollen. Klicken Sie auf **OK** und auf **Übernehmen**.

i. Kehren Sie zur Funktionsansicht des virtuellen Verzeichnisses **MESynchAgent** zurück, und doppelklicken Sie auf **BITS-Uploads**.

j. Wählen Sie **Clients können Dateien hochladen** und **Standardeinstellungen des übergeordneten Elements verwenden** aus. Klicken Sie auf **Übernehmen**.

IIS 6.0

a. Klicken Sie in der **Internet Information Services (IIS) Manager**-Konsole mit der rechten Maustaste auf die Standardwebsite, und wählen Sie **Neu > Virtuelles Verzeichnis** aus.

b. Geben Sie im **Assistenten zum Erstellen eines virtuellen Verzeichnisses** den Alias `MESynchAgent` für das virtuelle Verzeichnis ein, und klicken Sie auf **Weiter**.

c. Legen Sie einen Pfad fest, unter dem der Inhalt für dieses virtuelle Verzeichnis gespeichert werden soll, und klicken Sie auf **Weiter**.

> **HINWEIS**
>
> Merken Sie sich den konfigurierten Pfad für eine spätere Verwendung.

d. Aktivieren Sie die Kontrollkästchen **Lesen** und **Schreiben**, und deaktivieren Sie alle anderen Kontrollkästchen. Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.

e. Klicken Sie mit der rechten Maustaste auf das virtuelle Verzeichnis **MESynchAgent**, und wählen Sie **Eigenschaften** aus.

f. Wechseln Sie zur Registerkarte **Verzeichnissicherheit**, und klicken Sie in der Gruppe **Authentifizierung und Zugriffssteuerung** auf **Bearbeiten**.

g. Aktivieren Sie in der Gruppe **Authentifizierter Zugriff** die Option **Standardauthentifizierung**, und legen Sie die **Standarddomäne** und den **Bereich** für Benutzername und Kennwort fest, die von Slave-Rechnern für die Authentifizierung verwendet werden sollen.

> **HINWEIS**
>
> Alle anderen Kontrollkästchen dürfen nicht aktiviert sein.

h. Klicken Sie auf **OK**.

i. Aktivieren Sie auf der Registerkarte **BITS-Servererweiterung** das Kontrollkästchen **Datenübertragung in dieses virtuelle Verzeichnis durch Clients zulassen**.

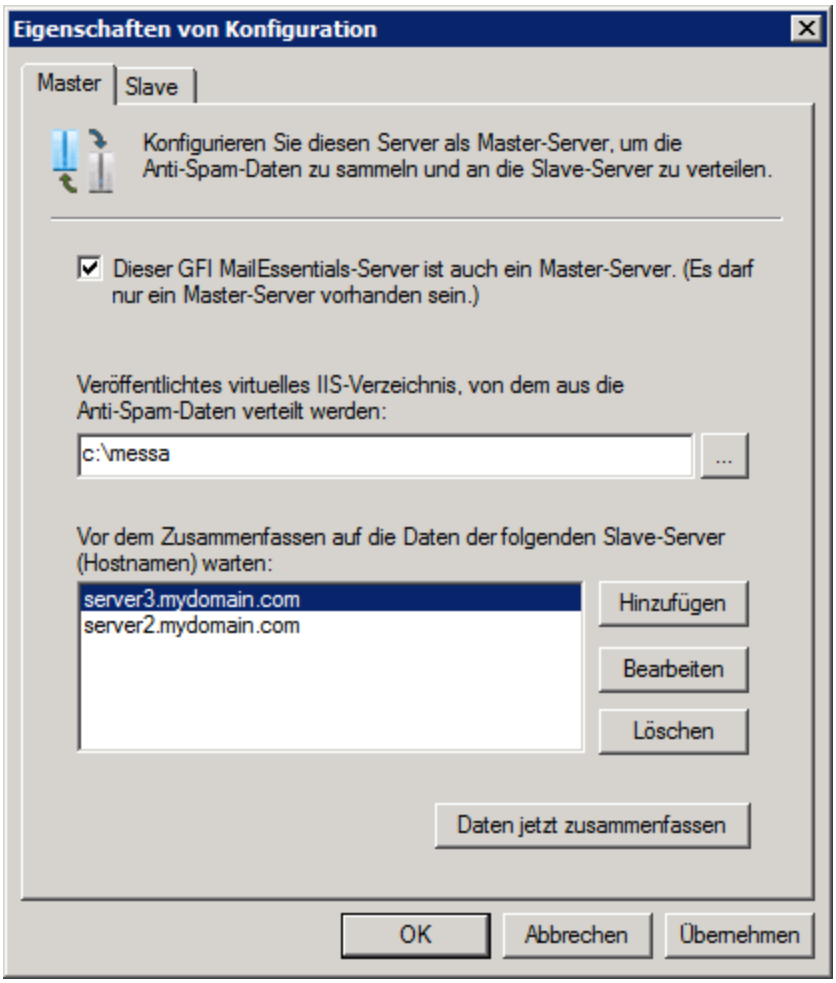
j. Klicken Sie auf **OK**, um das Eigenschaftendialogfeld des virtuellen Verzeichnisses zu schließen.

Schritt 2: Konfigurieren des GFI MailEssentials-Master-Servers

1. Navigieren Sie auf dem Master-Server zu <*GFI MailEssentials*

Installationspfad>\GFI\MailEssentials\AntiSpam\, und öffnen Sie **mesentcfg.msc**.

2. Klicken Sie mit der rechten Maustaste auf **Anti-Spam-Synchronisationsagent > Konfiguration** und wählen Sie **Eigenschaften** aus.



Screenshot 140: Konfigurieren eines Master-Servers

3. Aktivieren Sie auf der Registerkarte **Master** das Kontrollkästchen **Dieser GFI MailEssentials Configuration-Server ist auch ein Master-Server**, und geben Sie den vollständigen Pfad des Ordners ein, in dem der Inhalt des virtuellen Verzeichnisses **MESynchAgent** gespeichert werden soll.

4. Klicken Sie auf **Hinzufügen**, und geben Sie den Hostnamen des Slave-Servers ein. Klicken Sie auf **OK**, um ihn der Liste hinzuzufügen. Wiederholen Sie diesen Schritt, um alle anderen Slave-Server hinzuzufügen.

HINWEIS

Alle Computer, die der Liste hinzugefügt werden, müssen als Slave-Server konfiguriert werden. Andernfalls kann der Synchronisationsagent auf dem Master-Server die Daten nicht zusammenführen.

HINWEIS

Ein Master-Server kann auch gleichzeitig ein Slave-Server sein. In diesem Fall führt der Server seine eigenen Daten ebenfalls mit den hochgeladenen Daten der anderen Slave-Server zusammen. Fügen Sie hierfür den Hostnamen des Master-Servers der Liste der Slave-Server hinzu.

5. Wenn Sie einen Slave-Server bearbeiten oder löschen möchten, wählen Sie ihn in der Liste aus, und klicken Sie auf **Bearbeiten** oder **Löschen**.

6. Klicken Sie auf **OK**.

Schritt 3: Konfigurieren der Slave-Server

Wichtige Hinweise

1. Slave-Server müssen eine der folgenden Spezifikationen aufweisen:

» Microsoft® Windows Server 2008

» Microsoft® Windows Server 2003 – Es wird empfohlen, das BITS 2.0-Client-Update hier herunterzuladen:

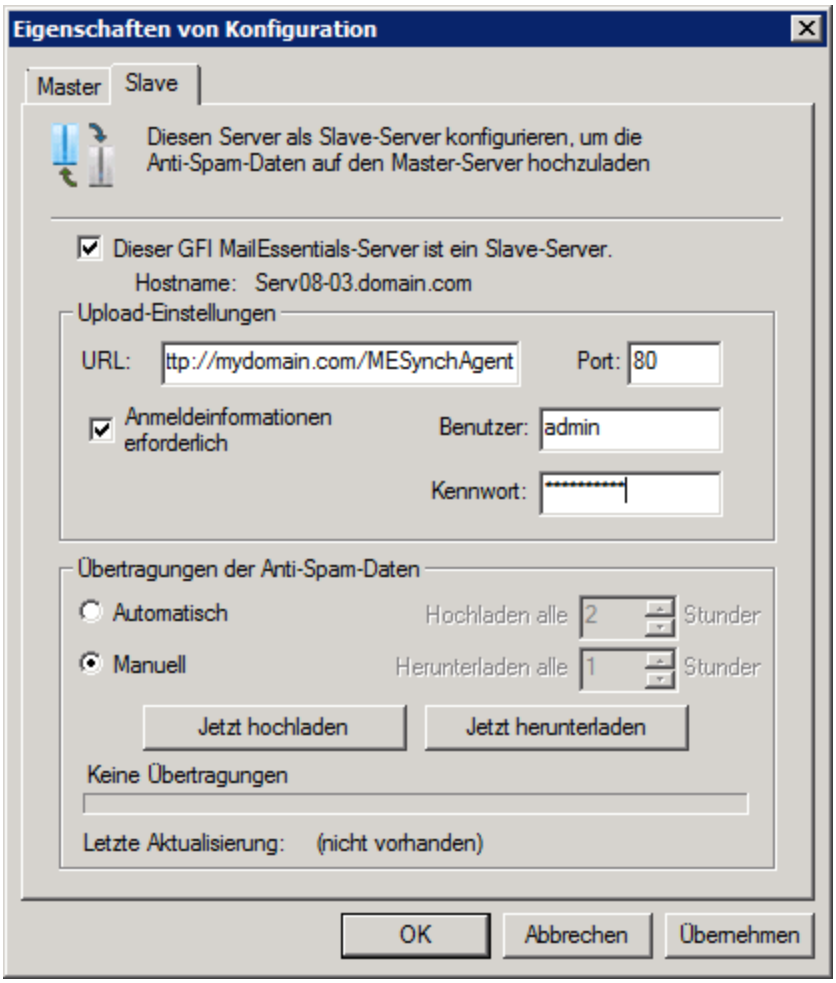
http://go.gfi.com/?pageid=ME_BITS2003Update

2. Von den Slave-Servern wird automatisch eine Archivdatei mit Einstellungen in das virtuelle IIS-Verzeichnis auf dem Master-Server hochgeladen. Aus diesem Grund sollten auf den Slave-Servern keine virtuellen Verzeichnisse erstellt werden.

Konfigurieren eines Slave-Servers

1. Navigieren Sie auf dem Slave-Server zu <*GFI MailEssentials Installationspfad*>\GFI\MailEssentials\`AntiSpam\`, und öffnen Sie **mesentcfg.msc**.

2. Klicken Sie mit der rechten Maustaste auf **Anti-Spam-Synchronisationsagent > Konfiguration** und wählen Sie **Eigenschaften** aus.



Screenshot 141: Konfigurieren eines Slave-Servers

3. Aktivieren Sie auf der Registerkarte **Slave** die Option **Dieser GFI MailEssentials-Server ist ein Slave-Server**.

4. Geben Sie im URL-Feld die vollständige URL für das virtuelle Verzeichnis auf dem Master-Server im folgenden Format ein:

`http://<Domänenname des Master-Servers>/MESynchAgent`

» Beispiel: `http://mydomain.com/MESynchAgent`

5. Geben Sie im Feld **Port** den Port ein, den der Master-Server für die HTTP-Kommunikation verwendet.

> **HINWEIS**
>
> Als Vorgabe ist bereits der standardmäßige HTTP-Port **80** angegeben.

6. Wählen Sie **Anmeldeinformationen erforderlich** aus, und geben Sie die Anmeldeinformationen für die Authentifizierung beim Master-Server ein.

7. Wählen Sie die gewünschte Option aus:

Option	Beschreibung
Automatisch	Die Synchronisierung erfolgt automatisch in einem festgelegten Intervall. Geben Sie im Feld **Hochladen alle** an, in welchem zeitlichen Abstand (in Stunden) der Slave-Server seine Einstellungen auf den Master-Server hochladen soll. Geben Sie im Feld **Herunterladen alle** an, in welchem zeitlichen Abstand (in Stunden) der Slave-Server nach Aktualisierungen auf dem Master-Server suchen und diese herunterladen soll. Wichtige Hinweise zum Festlegen des Intervalls: » Upload- und Download-Intervall müssen unterschiedlich sein. » Es kann ein stündliches Intervall zwischen 1 und 240 Stunden angegeben werden. » Es wird empfohlen, für das Download-Intervall einen kleineren Wert festzulegen als für das Upload-Intervall. » Es wird empfohlen, für alles Slave-Server dasselbe Intervall zu verwenden. Beispiel: Stellen Sie das Download-Intervall auf 3 Stunden und das Upload-Intervall auf 4 Stunden ein. Auf diese Weise finden Downloads häufiger statt als Uploads.
Manuell	Die Archivdatei mit den Einstellungen wird manuell hoch- und heruntergeladen. Um die Einstellungen vom Slave-Server auf den Master-Server hochzuladen, klicken Sie auf **Jetzt hochladen**. Um die aktualisierten, zusammengeführten Einstellungen vom Master-Server herunterzuladen, klicken Sie auf **Jetzt herunterladen**.

8. Klicken Sie auf **OK**.

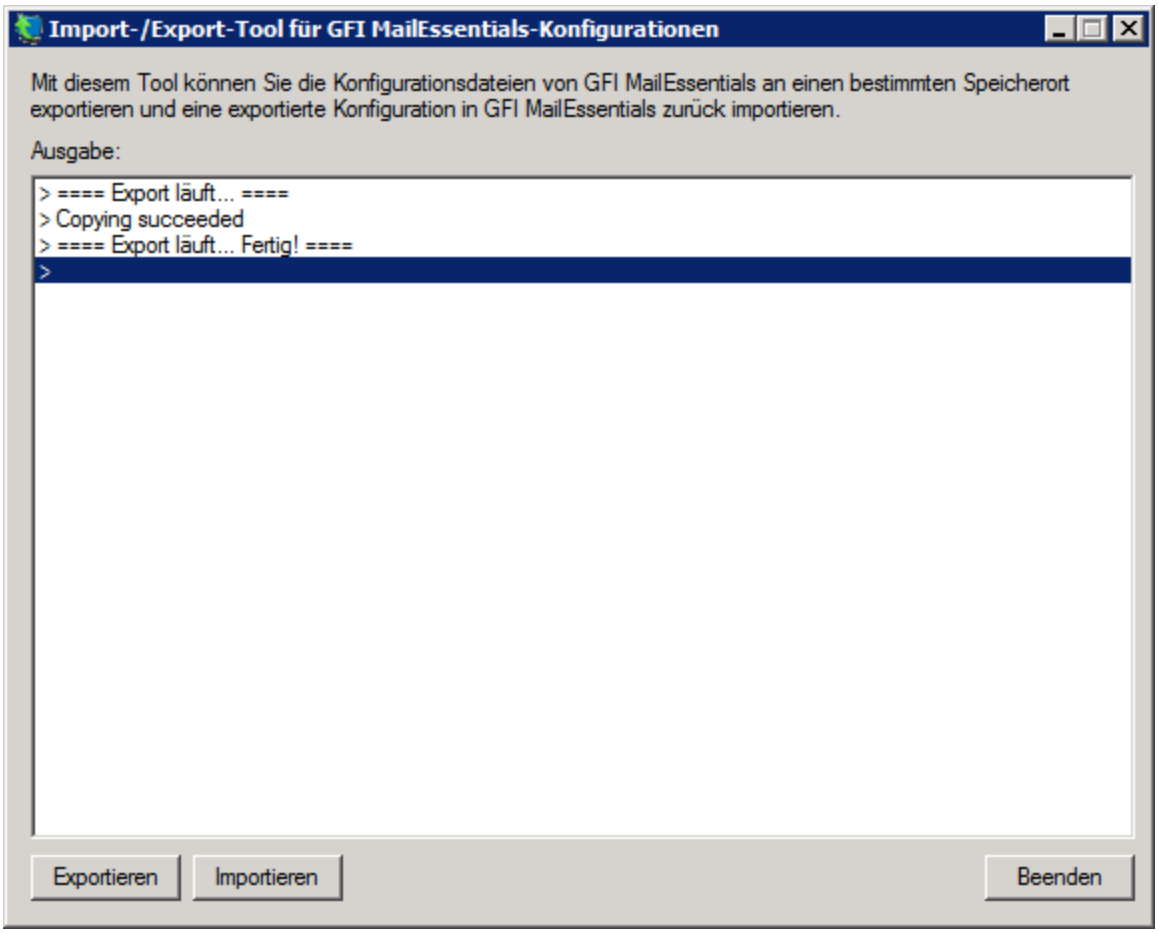
11.9.2 Manuelles Exportieren und Importieren von Einstellungen

GFI MailEssentials beinhaltet ein Import-/Export-Tool für Konfigurationseinstellungen, mit dem die Einstellungen aus einer Installation exportiert und in eine andere importiert werden können.

> **HINWEIS**
>
> Die Einstellungen können auch über die Befehlszeile importiert/exportiert werden. Weitere Informationen finden Sie unter „Exportieren/Importieren von Einstellungen über die Befehlszeile“ (Seite 278).

Schritt 1: Exportieren der vorhandenen Einstellungen

1. Navigieren Sie zu `<GFI MailEssentials Installationspfad>\GFI\MailEssentials\`, und starten Sie **meconfigmgr.exe**.


Import-/Export-Tool für GFI MailEssentials-Konfigurationen
Mit diesem Tool können Sie die Konfigurationsdateien von GFI MailEssentials an einen bestimmten Speicherort exportieren und eine exportierte Konfiguration in GFI MailEssentials zurück importieren.
Ausgabe:
> ==== Export läuft... ====
> Copying succeeded
> ==== Export läuft... Fertig! ====
>
Exportieren
Importieren
Beenden

Screenshot 142: Import-/Export-Tool für Konfigurationseinstellungen

> **HINWEIS**
>
> Die Dauer des Exportvorgangs hängt von der Größe der Datenbank ab.

4. Klicken Sie auf **Exportieren**.

5. Wählen Sie im Dialogfeld **Nach Ordner suchen** den Ordner aus, in den die Konfigurationseinstellungen exportiert werden sollen, und klicken Sie auf **OK**.

6. Klicken Sie nach Abschluss auf **Beenden**.

Schritt 2: Kopieren der exportierten Einstellungen

1. Kopieren Sie manuell den Ordner, in den die Konfigurationseinstellungen exportiert wurden.

2. Fügen Sie den Ordner auf dem Rechner ein, wo die Einstellungen importiert werden sollen.

Schritt 3: Importieren von Einstellungen in die neue Installation

> **WICHTIG**
>
> Beim Importieren von Einstellungen werden die bestehenden Einstellungen (z. B. Quell-DNS-Einstellungen) von den importierten Dateien überschrieben. Dadurch ist wahrscheinlich eine Neukonfiguration von bestimmten Netzwerkeinstellungen und Spam-Aktionen erforderlich.

HINWEIS

Einige Dienste werden vorübergehend angehalten, während dieser Vorgang ausgeführt wird. Dies kann den E-Mail-Fluss und/oder die E-Mail-Scans beeinträchtigen.

1. Halten Sie die folgenden Dienste an:

» GFI List Server

» GFI MailEssentials Enterprise-Übertragung

» GFI MailEssentials Legacy Attendant

» GFI MailEssentials AntiSpam Attendant

» GFI POP2Exchange

» IIS Admin-Dienst

2. Navigieren Sie zu *<GFI MailEssentials Installationspfad>*\GFI\MailEssentials\, und starten Sie **meconfigmgr.exe**.

HINWEIS

Die Dauer des Importvorgangs hängt von der Größe der importierten Datenbank ab.

4. Klicken Sie auf **Importieren**, wählen Sie den Ordner mit den Importdaten aus, und klicken Sie auf **OK**.

WARNHINWEIS

Beim Importvorgang werden die Konfigurationsdateien von den Dateien dieses Ordners überschrieben.

HINWEIS

Einige importierte Einstellungen sind möglicherweise nicht für die Installation von GFI MailEssentials geeignet und müssen neu konfiguriert werden. Dies ist beispielsweise der Fall, wenn DNS-Einstellungen, Domänenlisten und Perimeter-Server auf dem Server, von dem die Einstellungen exportiert wurden, unterschiedlich sind. Klicken Sie auf **Ja**, um den Nachinstallationsassistenten von GFI MailEssentials zu starten. Dieser konfiguriert wichtige Einstellungen neu.

Weitere Informationen finden Sie unter „Nachinstallationsassistent“ (Seite 43).

Es wird außerdem empfohlen, die folgenden Einstellungen zu überprüfen, die nicht mit dem Nachinstallationsassistenten konfiguriert werden.

» **Directory Harvesting** – Dies muss beim Import auf einen Server überprüft werden, der mit einem anderen Active Directory oder mit einem Active Directory auf einem anderen Server verbunden ist. Weitere Informationen finden Sie unter „Directory Harvesting“ (Seite 117).

» **Spam-Aktionen** – Einige Spam-Aktionen sind nur für Microsoft® Exchange-Umgebungen verfügbar. Diese Aktionen funktionieren nicht, wenn die Einstellungen in eine andere Umgebung (z. B. auf einen IIS-Server) importiert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

HINWEIS

Weitere Informationen zu Einstellungen, die nach dem Import geprüft werden sollten, finden Sie unter:

http://go.gfi.com/?pageid=ME_CheckImportSettings

6. Klicken Sie nach Abschluss auf **Beenden**.

7. GFI MailEssentials versucht automatisch, die in Schritt 1 angehaltenen Dienste wieder zu starten.

WICHTIG

Beim Anhalten des **IIS Admin-Dienstes** werden möglicherweise auch andere Dienste angehalten, z. B. der **Simple Mail Transfer Protocol (SMTP)**-Dienst. Diese Dienste können Sie im Dienste-Applet manuell neu starten.

11.9.3 Exportieren/Importieren von Einstellungen über die Befehlszeile

Exportieren von Einstellungen über die Befehlszeile

1. Halten Sie die folgenden GFI MailEssentials-Dienste an:

» GFI MailEssentials AS-Scan-Engine

» GFI MailEssentials AS Attendant

2. Wechseln Sie in der Eingabeaufforderung zum Installationsstammverzeichnis von GFI MailEssentials.

3. Geben Sie Folgendes ein:

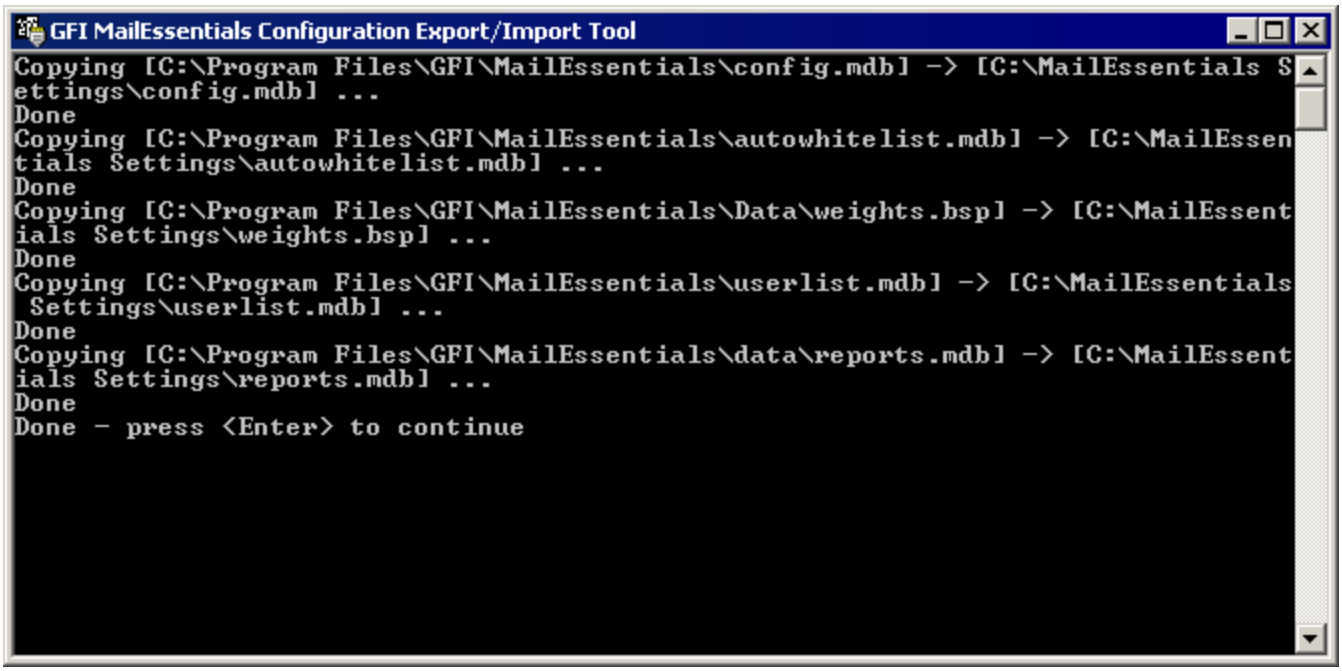
```
meconfigmgr /export:"c:\MailEssentials Settings" /verbose /replace
```

Bedeutung der Parameter:

» `"C:\MailEssentials Settings"` - Speicherort, an den die Dateien exportiert werden sollen. Ersetzen Sie dies mit dem gewünschten Pfad.

» `/verbose` - Weist das Tool an, beim Kopieren der Dateien den Fortschritt anzuzeigen.

» `/replace` - Weist das Tool an, vorhandene Dateien im Zielordner zu überschreiben.


GFI MailEssentials Configuration Export/Import Tool
Copying [C:\Program Files\GFI\MailEssentials\config.mdb] -> [C:\MailEssentials Settings\config.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\autowhitelist.mdb] -> [C:\MailEssentials Settings\autowhitelist.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\Data\weights.bsp] -> [C:\MailEssentials Settings\weights.bsp] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\userlist.mdb] -> [C:\MailEssentials Settings\userlist.mdb] ...
Done
Copying [C:\Program Files\GFI\MailEssentials\data\reports.mdb] -> [C:\MailEssentials Settings\reports.mdb] ...
Done
Done - press <Enter> to continue

Screenshot 143: Exportieren von Einstellungen über die Befehlszeile

4. Starten Sie die Dienste erneut, die Sie in Schritt 1 angehalten haben.

Importieren von Einstellungen über die Befehlszeile

1. Halten Sie die folgenden Dienste an:

» GFI List Server

» GFI MailEssentials Enterprise-Übertragung

» GFI MailEssentials Legacy Attendant

» GFI MailEssentials AntiSpam Attendant

» GFI POP2Exchange

» IIS Admin-Dienst

2. Wechseln Sie in der Eingabeaufforderung zum Installationsstammverzeichnis von GFI MailEssentials.

3. Geben Sie Folgendes ein:

```
meconfigmgr /import:"c:\MailEssentials Settings" /verbose /replace
```

Bedeutung der Parameter:

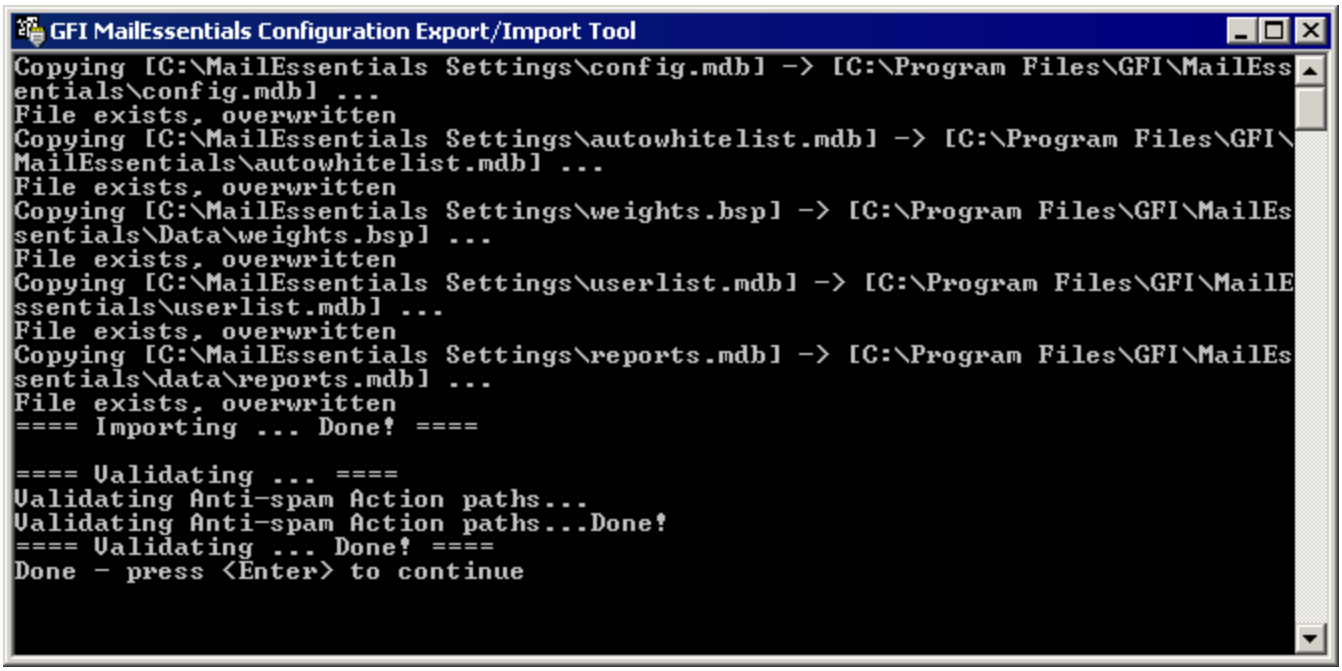
» `"C:\MailEssentials Settings"` - Speicherort, an dem sich die Dateien befinden, die importiert werden sollen. Ersetzen Sie dies mit dem Pfad, unter dem sich die Dateien für den Import befinden.

» `/verbose` - Weist das Tool an, beim Kopieren der Dateien den Fortschritt anzuzeigen.

» `/replace` - Weist das Tool an, vorhandene Dateien im Zielordner zu überschreiben.

WARNHINWEIS

Beim Importvorgang werden die Konfigurationsdateien von den Dateien dieses Ordners überschrieben.


GFI MailEssentials Configuration Export/Import Tool
Copying [C:\MailEssentials Settings\config.mdb] -> [C:\Program Files\GFI\MailEss
entials\config.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\autowhitelist.mdb] -> [C:\Program Files\GFI\
MailEssentials\autowhitelist.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\weights.bsp] -> [C:\Program Files\GFI\MailEs
sentials\Data\weights.bsp] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\userlist.mdb] -> [C:\Program Files\GFI\MailE
ssentials\userlist.mdb] ...
File exists, overwritten
Copying [C:\MailEssentials Settings\reports.mdb] -> [C:\Program Files\GFI\MailEs
sentials\data\reports.mdb] ...
File exists, overwritten
==== Importing ... Done! ====
==== Validating ... ====
Validating Anti-spam Action paths...
Validating Anti-spam Action paths...Done!
==== Validating ... Done! ====
Done - press <Enter> to continue

Screenshot 144: Importieren von Einstellungen über die Befehlszeile

4. Starten Sie die Dienste erneut, die Sie in Schritt 1 angehalten haben.

HINWEIS

Einige importierte Einstellungen sind möglicherweise nicht für die Installation von GFI MailEssentials geeignet und müssen neu konfiguriert werden. Dies ist beispielsweise der Fall, wenn DNS-Einstellungen, Domänenlisten und Perimeter-Server auf dem Server, von dem die Einstellungen exportiert wurden, unterschiedlich sind. Klicken Sie auf **Ja**, um den Nachinstallationsassistenten von GFI MailEssentials zu starten. Dieser konfiguriert wichtige Einstellungen neu.

Weitere Informationen finden Sie unter „Nachinstallationsassistent“ (Seite 43).

Es wird außerdem empfohlen, die folgenden Einstellungen zu überprüfen, die nicht mit dem Nachinstallationsassistenten konfiguriert werden.

» **Directory Harvesting** – Dies muss beim Import auf einen Server überprüft werden, der mit einem anderen Active Directory oder mit einem Active Directory auf einem anderen Server verbunden ist. Weitere Informationen finden Sie unter „Directory Harvesting“ (Seite 117).

» **Spam-Aktionen** – Einige Spam-Aktionen sind nur für Microsoft® Exchange-Umgebungen verfügbar. Diese Aktionen funktionieren nicht, wenn die Einstellungen in eine andere Umgebung (z. B. auf einen IIS-Server) importiert werden. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150).

HINWEIS

Weitere Informationen zu Einstellungen, die nach dem Import geprüft werden sollten, finden Sie unter:

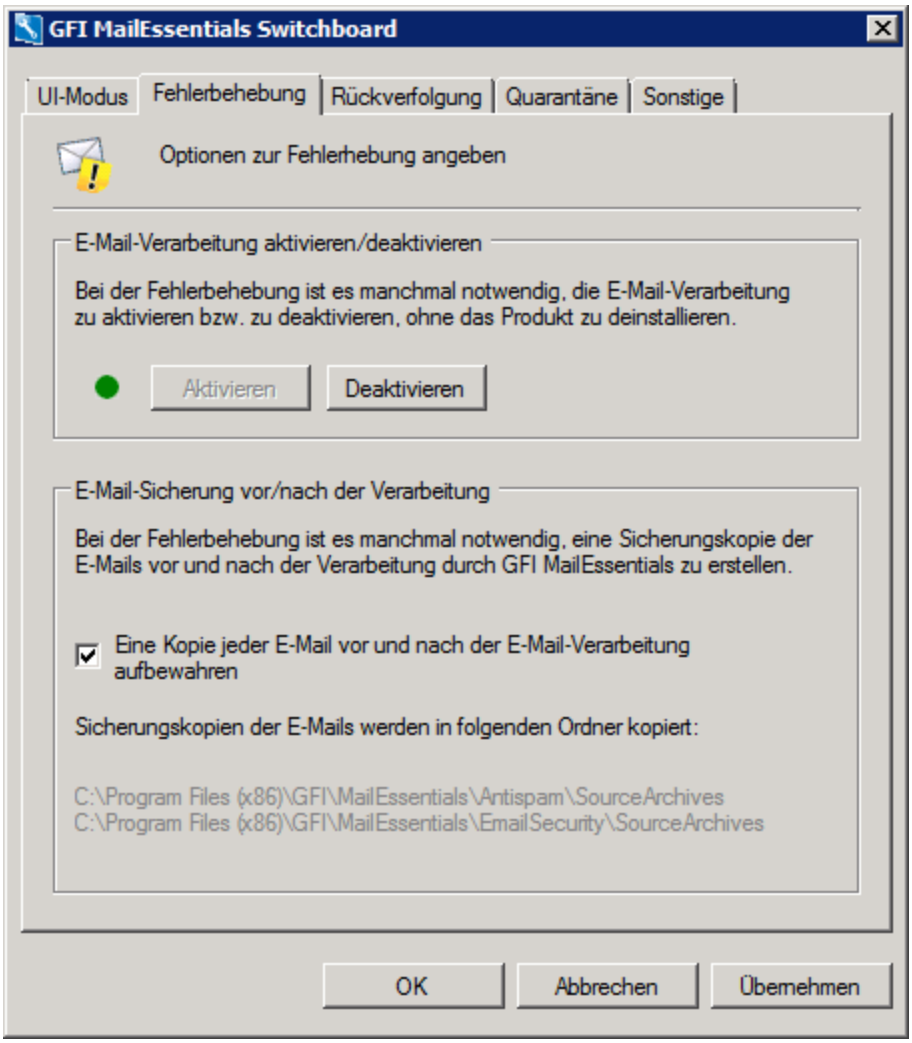
http://go.gfi.com/?pageid=ME_CheckImportSettings

11.10 Deaktivieren der E-Mail-Verarbeitung

Wenn Sie die E-Mail-Verarbeitung deaktivieren, werden alle Schutzmechanismen von GFI MailEssentials deaktiviert, und alle E-Mails (einschließlich Spam und schädlicher E-Mails) gelangen in die Postfächer Ihrer Benutzer. Üblicherweise wird die E-Mail-Verarbeitung nur zu Fehlerbehebungszwecken deaktiviert.

So aktivieren/deaktivieren Sie die Verarbeitung von E-Mails durch GFI MailEssentials:

1. Starten Sie das GFI MailEssentials Switchboard über **Start > Programme > GFI MailEssentials > Switchboard**, und wählen Sie die Registerkarte **Fehlerbehebung** aus.


GFI MailEssentials Switchboard
UI-Modus
Fehlerbehebung
Rückverfolgung
Quarantäne
Sonstige
Optionen zur Fehlerhebung angeben
E-Mail-Verarbeitung aktivieren/deaktivieren
Bei der Fehlerbehebung ist es manchmal notwendig, die E-Mail-Verarbeitung zu aktivieren bzw. zu deaktivieren, ohne das Produkt zu deinstallieren.
Aktivieren
Deaktivieren
E-Mail-Sicherung vor/nach der Verarbeitung
Bei der Fehlerbehebung ist es manchmal notwendig, eine Sicherungskopie der E-Mails vor und nach der Verarbeitung durch GFI MailEssentials zu erstellen.
Eine Kopie jeder E-Mail vor und nach der E-Mail-Verarbeitung aufbewahren
Sicherungskopien der E-Mails werden in folgenden Ordner kopiert:
C:\Program Files (x86)\GFI\MailEssentials\Antispam\SourceArchives
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\SourceArchives
OK
Abbrechen
Übernehmen

Screenshot 145: Das GFI MailEssentials Switchboard: Fehlerbehebung

2. Klicken Sie auf **Aktivieren** oder **Deaktivieren**, um die E-Mail-Verarbeitung zu aktivieren/deaktivieren.

> **HINWEIS**
>
> Einige Dienste werden vorübergehend angehalten, während dieser Vorgang ausgeführt wird. Dies kann den E-Mail-Fluss und/oder die E-Mail-Scans beeinträchtigen.

3. Klicken Sie im Dialogfeld **Dienstneustart erforderlich** auf **Ja**, um die Dienste neu zu starten.

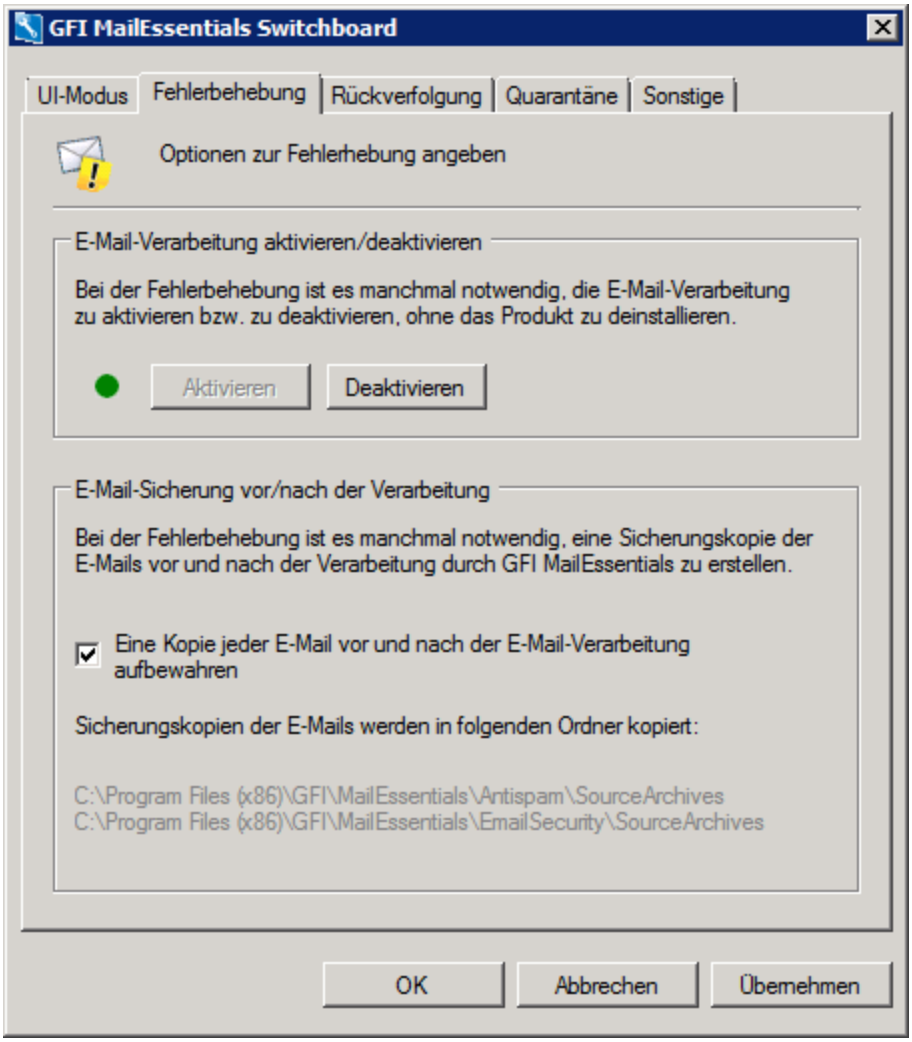
4. Klicken Sie auf **OK**.

11.11 E-Mail-Sicherung vor und nach der Verarbeitung

WICHTIG

Diese Option ist nur für Fehlerbehebungszwecke vorgesehen.

1. Starten Sie das GFI MailEssentials Switchboard über **Start > Programme > GFI MailEssentials > Switchboard**, und wählen Sie die Registerkarte **Fehlerbehebung** aus.


GFI MailEssentials Switchboard
UI-Modus
Fehlerbehebung
Rückverfolgung
Quarantäne
Sonstige
Optionen zur Fehlerhebung angeben
E-Mail-Verarbeitung aktivieren/deaktivieren
Bei der Fehlerbehebung ist es manchmal notwendig, die E-Mail-Verarbeitung zu aktivieren bzw. zu deaktivieren, ohne das Produkt zu deinstallieren.
Aktivieren
Deaktivieren
E-Mail-Sicherung vor/nach der Verarbeitung
Bei der Fehlerbehebung ist es manchmal notwendig, eine Sicherungskopie der E-Mails vor und nach der Verarbeitung durch GFI MailEssentials zu erstellen.
Eine Kopie jeder E-Mail vor und nach der E-Mail-Verarbeitung aufbewahren
Sicherungskopien der E-Mails werden in folgenden Ordner kopiert:
C:\Program Files (x86)\GFI\MailEssentials\Antispam\SourceArchives
C:\Program Files (x86)\GFI\MailEssentials\EmailSecurity\SourceArchives
OK
Abbrechen
Übernehmen

Screenshot 146: Das GFI MailEssentials Switchboard: Fehlerbehebung

2. Wählen Sie **Eine Kopie jeder E-Mail vor und nach der E-Mail-Verarbeitung aufbewahren** aus, um eine Kopie jeder verarbeiteten E-Mail zu speichern.

Alle E-Mails werden an den folgenden Speicherorten aufbewahrt:

» *<GFI MailEssentials Installationspfad>*\GFI\MailEssentials\AntiSpam\SourceArchives\

» *<GFI MailEssentials Installationspfad>*\GFI\MailEssentials\EmailSecurity\SourceArchives\

HINWEIS

Einige Dienste werden vorübergehend angehalten, während dieser Vorgang ausgeführt wird. Dies kann den E-Mail-Fluss und/oder die E-Mail-Scans beeinträchtigen.

3. Klicken Sie auf **OK**.

4. Klicken Sie im Dialogfeld **Dienstneustart erforderlich** auf **Ja**, um die Dienste neu zu starten.

5. Klicken Sie auf **OK**.

11.12 Fernzugriffsports

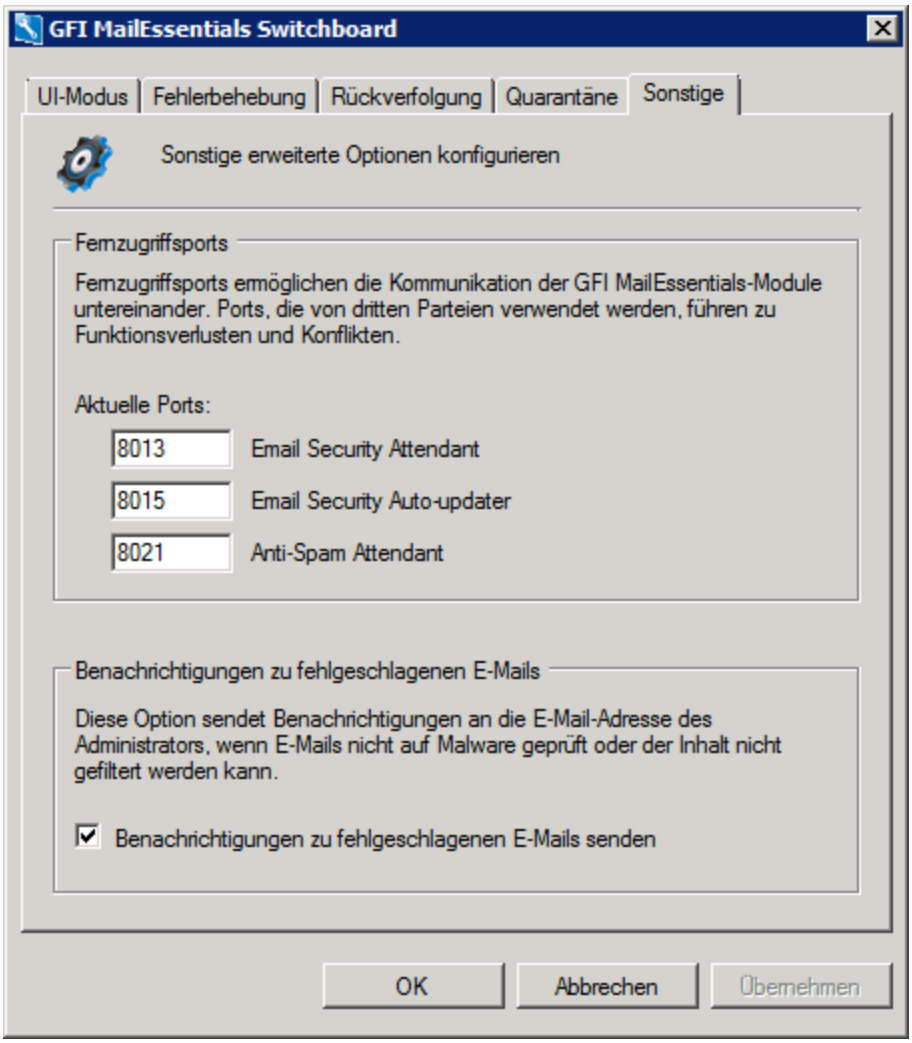
Fernzugriffsports ermöglichen die Kommunikation der GFI MailEssentials-Module untereinander. Standardmäßig verwendet GFI MailEssentials folgende Ports:

- 8013
- 8015
- 8021

Stellen Sie sicher, dass keine anderen Anwendungen (außer GFI MailEssentials) diese Ports abhören. Werden diese Ports von anderen Anwendungen verwendet, definieren Sie für GFI MailEssentials andere Ports.

So ändern Sie die Fernzugriffsports:

1. Starten Sie das GFI MailEssentials Switchboard über **Start > Programme > GFI MailEssentials > Switchboard**, und wählen Sie die Registerkarte **Weitere** aus.



Screenshot 147: Ändern von Fernzugriffsports

2. Ändern Sie im Bereich **Fernzugriffsports** die Nummer des betreffenden Fernzugriffsports in eine Nummer, die nicht von anderen Anwendungen verwendet wird.

3. Klicken Sie auf **Übernehmen**.

> **HINWEIS**
>
> Einige Dienste werden vorübergehend angehalten, während dieser Vorgang ausgeführt wird. Dies kann den E-Mail-Fluss und/oder die E-Mail-Scans beeinträchtigen.

4. Klicken Sie auf **Ja**, um die angezeigten Dienste neu zu starten.

5. Klicken Sie auf **OK**.

11.13 Überwachen der Virus Scanning API

Wenn GFI MailEssentials auf dem Microsoft® Exchange-Rechner installiert ist, können Sie die Leistung der Virus Scanning API mithilfe der Systemmonitor-MMC überwachen.

> **HINWEIS**
>
> Informationsspeicherschutz (VSAPI) wird unter Microsoft® Exchange Server 2013 nicht unterstützt, da Microsoft VSAPI von Microsoft® Exchange Server 2013 entfernt hat.

11.13.1 Leistungsindikator in Windows 2003 Server

Führen Sie folgende Schritte aus, um einen Leistungsindikator in Windows 2003 Server hinzuzufügen und anzuzeigen:

1. Wählen Sie **Start > Systemsteuerung** aus.

2. Doppelklicken Sie in der Systemsteuerung auf **Verwaltung**.

3. Doppelklicken Sie auf **Leistung**, um die **Systemmonitor**-MMC zu starten.

4. Klicken Sie im Anzeigebereich **Systemmonitor** auf **Hinzufügen**, um das Dialogfeld **Leistungsindikatoren hinzufügen** zu laden.

5. Wählen Sie in der Dropdown-Liste **Leistungsobjekt** den Eintrag **MSExchangeIS** aus.

6. Klicken Sie auf **Leistungsindikatoren wählen**.

7. Wählen Sie einen **Virenscanner**-Leistungsindikator aus, den Sie hinzufügen möchten. Weitere Informationen finden Sie unter „Leistungsindikatoren“ (Seite 287).

8. Klicken Sie auf **Hinzufügen**.

9. Wiederholen Sie die Schritte 7 und 8, um alle benötigten Leistungsindikatoren hinzuzufügen.

10. Klicken Sie auf **Schließen**.

Die Leistungsindikatoren für die hinzugefügten Prozesse werden nun im Systemmonitor angezeigt.

11.13.2 Leistungsindikator in Windows 2008 Server

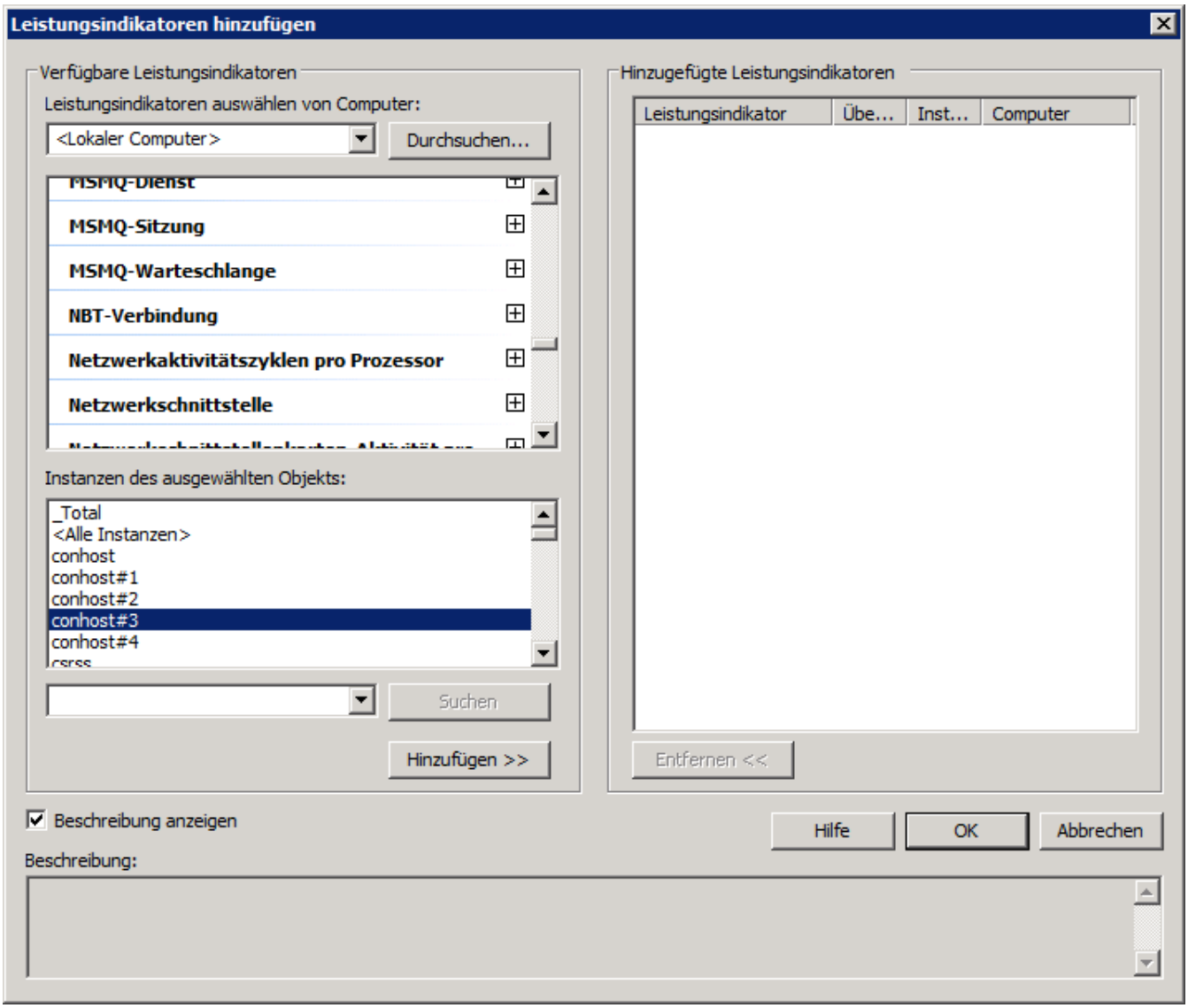
> **HINWEIS**
>
> In einer Microsoft® Exchange Server 2007/2010-Umgebung sind die VSAPI-Leistungsindikatoren nur auf Rechnern verfügbar, auf denen die Postfachserverrolle installiert ist.

Führen Sie folgende Schritte aus, um einen Leistungsindikator in Windows 2008 Server hinzuzufügen und anzuzeigen:

1. Navigieren Sie zu **Start > Systemsteuerung > Verwaltung > Zuverlässigkeits- und Leistungsüberwachung**.

2. Erweitern Sie im Überwachungsdialogfeld den Punkt **Überwachungstools**, und wählen Sie **Systemmonitor** aus.

3. Klicken Sie im Anzeigebereich auf **Hinzufügen**, um das Dialogfeld **Leistungsindikatoren hinzufügen** zu laden.



Screenshot 148: Hinzufügen von Leistungsindikatoren für die VSAPI in Windows 2008 Server

4. Wählen Sie in der Dropdown-Liste **Leistungsindikatoren auswählen von Computer** den Computer aus, der überwacht werden soll.

5. Erweitern Sie in der Liste der verfügbaren Leistungsindikatoren den Eintrag **MSExchangeIS**.

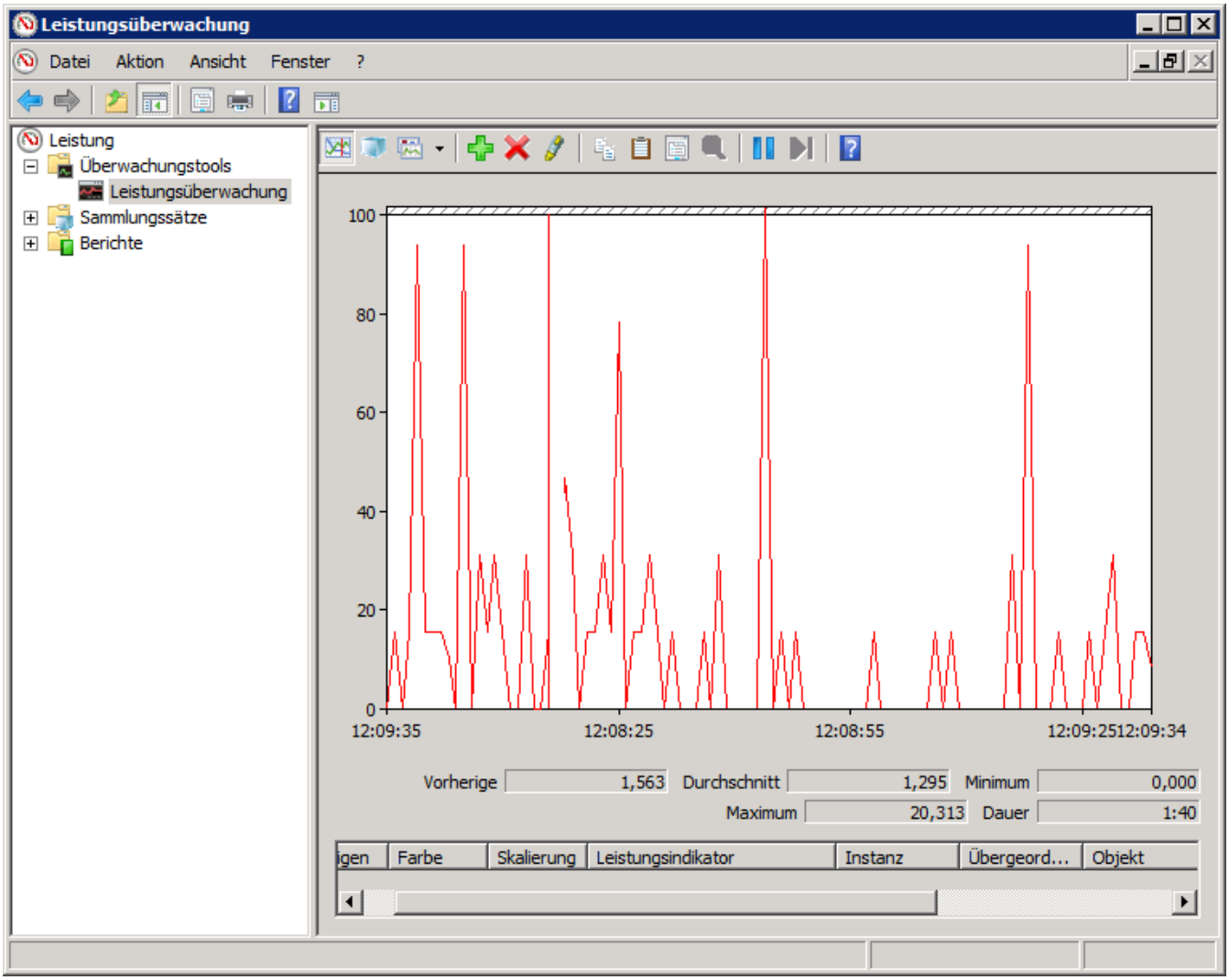
6. Wählen Sie einen **Virenscanner**-Leistungsindikator aus, den Sie hinzufügen möchten. Weitere Informationen finden Sie unter „Leistungsindikatoren“ (Seite 287).

7. Klicken Sie auf **Hinzufügen**.

8. Wiederholen Sie die Schritte 6 und 7 für jeden Prozess, der überwacht werden soll.

9. Klicken Sie auf **OK**, um die Änderungen zu übernehmen.

Die Leistungsindikatoren für die hinzugefügten Prozesse werden nun im Systemmonitor angezeigt.



Screenshot 149: Überwachung von 'Virenscanner - Gescannte Dateien' im Systemmonitor von Windows Server 2008

11.13.3 Leistungsindikatoren

Folgende Leistungsindikatoren für die VSAPI sind verfügbar:

Leistungsindikator	Beschreibung
Virenscanner - Verarbeitete Nachrichten	Die kumulative Gesamtanzahl der vom Virenscanner verarbeiteten Nachrichten der höchsten Ebene.
Virenscanner - Verarbeitete Nachrichten/Sek.	Die Geschwindigkeit, mit der Nachrichten der höchsten Ebene vom Virenscanner verarbeitet werden.
Virenscanner - Desinfizierte Nachrichten	Die Gesamtanzahl der vom Virenscanner desinfizierten Nachrichten der höchsten Ebene.
Virenscanner - Desinfizierte Nachrichten/Sek.	Die Geschwindigkeit, mit der Nachrichten der höchsten Ebene vom Virenscanner desinfiziert werden.
Virenscanner - Isolierte Nachrichten	Die Gesamtanzahl der Nachrichten der höchsten Ebene, die vom Virenscanner unter Quarantäne gestellt wurden.
Virenscanner - Isolierte Nachrichten/Sek.	Die Geschwindigkeit, mit der Nachrichten der höchsten Ebene vom Virenscanner unter Quarantäne gestellt werden.
Virenscanner - Gescannte Dateien	Die Gesamtanzahl der vom Virenscanner verarbeiteten, voneinander unabhängigen Dateien.
Virenscanner - Gescannte Dateien/Sek.	Die Geschwindigkeit, mit der voneinander unabhängige Dateien vom Virenscanner verarbeitet werden.

Leistungsindikator	Beschreibung
Virenscanner – Desinfizierte Dateien	Die Gesamtanzahl der vom Virenscanner desinfizierten, voneinander unabhängigen Dateien.
Virenscanner – Desinfizierte Dateien/Sek.	Die Geschwindigkeit, mit der voneinander unabhängige Dateien vom Virenscanner desinfiziert werden.
Virenscanner – Isolierte Dateien	Die Gesamtanzahl der voneinander unabhängigen Dateien, die vom Virenscanner unter Quarantäne gestellt wurden.
Virenscanner – Isolierte Dateien/Sek.	Die Geschwindigkeit, mit der voneinander unabhängige Dateien vom Virenscanner unter Quarantäne gestellt werden.
Virenscanner – Gescannte Bytes	Die Gesamtanzahl der Bytes in allen vom Virenscanner verarbeiteten Dateien.
Virenscanner – Warteschlangenlänge	Die aktuelle Anzahl ausstehender Anforderungen, die zum Virenscannen in die Warteschlange gestellt wurden.
Virenscanner – Im Hintergrund gescannte Ordner	Die Gesamtanzahl der im Hintergrund gescannten Ordner.
Virenscanner – Im Hintergrund gescannte Nachrichten	Die Gesamtanzahl der im Hintergrund gescannten Nachrichten.

12 Fehlerbehebung und Support

12.1 Einführung

In diesem Kapitel wird erklärt, wie bei der Installation von GFI MailEssentials auftretende Probleme behoben werden können. Die wichtigsten verfügbaren Informationsquellen zum Beheben dieser Probleme lauten wie folgt:

» Dieses Handbuch – die meisten Probleme können Sie mithilfe der Informationen in diesem Abschnitt lösen.

» Artikel aus der GFI Knowledge Base

» Webforum

» Technischer Support von GFI

12.2 Häufige Probleme

Aufgetretenes Problem	Lösung
Das Dashboard zeigt an, dass keine E-Mails verarbeitet werden oder dass nur eingehende oder ausgehende E-Mails verarbeitet werden.	1. Stellen Sie sicher, dass das Scannen von E-Mails in GFI MailEssentials nicht deaktiviert ist. Weitere Informationen finden Sie unter „Deaktivieren der E-Mail-Verarbeitung“ (Seite 281). 2. Überprüfen Sie, ob mehrere virtuelle Microsoft® IIS SMTP-Server vorhanden sind, und stellen Sie sicher, dass GFI MailEssentials an den richtigen virtuellen Server gebunden ist. Weitere Informationen finden Sie unter „Bindungen an virtuelle SMTP-Server“ (Seite 250). 3. Der MX-Eintrag für die Domäne ist nicht korrekt konfiguriert. Stellen Sie sicher, dass der MX-Eintrag auf die IP-Adresse des Servers verweist, auf dem GFI MailEssentials ausgeführt wird. 4. Wenn eingehende E-Mails über ein anderes Gateway weitergeleitet werden, stellen Sie sicher, dass der Mailserver, der am anderen Gateway ausgeführt wird, eingehende E-Mails über GFI MailEssentials weiterleitet. 5. Stellen Sie sicher, dass ausgehende E-Mails über GFI MailEssentials weitergeleitet werden. Weitere Informationen finden Sie unter „Installation auf einem Mail-Gateway- oder Relay-/Perimeter-Server“ (Seite 25). 6. Stellen Sie sicher, dass Microsoft® Exchange Server für ausgehende E-Mails den virtuellen SMTP-Server verwendet, an den GFI MailEssentials gebunden ist. Weitere Informationen zur Lösung dieses Problems finden Sie unter: http://go.gfi.com/?pageid=ME_MonitorProcessing
Nach der Installation von GFI MailEssentials wird in einigen E-Mails der Text fehlerhaft angezeigt, wenn sie in Microsoft® Outlook geöffnet werden.	Dieses Problem tritt bei E-Mails auf, die für den Header einen anderen Zeichensatz verwenden als für den Nachrichtentext. Wenn solche E-Mails von Microsoft® Exchange 2003 verarbeitet werden, werden sie in Microsoft® Outlook fehlerhaft angezeigt. Microsoft® hat einen Hotfix zur Behebung dieses Problems veröffentlicht. Weitere Informationen finden Sie unter: http://go.gfi.com/?pageid=ME_OutlookCharacters and http://go.gfi.com/?pageid=ME_MessageGarbled
GFI MailEssentials ist so konfiguriert, dass blockierte SPAM-E-Mails in einen Unterordner des Benutzerpostfachs verschoben werden. Clients, die über POP3 mit Microsoft® Exchange verbunden sind, können blockierte SPAM-E-Mails nicht anzeigen.	Verwenden Sie IMAP für die Verbindung mit Microsoft® Exchange. Weitere Informationen finden Sie unter: http://go.gfi.com/?pageid=ME_POP3ViewSpam

Aufgetretenes Problem	Lösung
Automatische Aktualisierungen schlagen fehl, aber das manuelle Herunterladen über GFI MailEssentials Configuration funktioniert problemlos.	Stellen Sie sicher, dass Verbindungen ohne Authentifizierung zwischen dem GFI MailEssentials-Rechner und http://update.gfi.com über Port 80 zulässig sind. Weitere Informationen finden Sie unter: http://go.gfi.com/?pageid=ME_AutoUpdatesFail Überprüfen Sie auch den Proxy-Server, falls vorhanden.
Konfigurationsdaten können nicht importiert werden.	Stellen Sie sicher, dass Version und Build von GFI MailEssentials auf der Quell- und Zielinstallation übereinstimmen. Weitere Informationen zur Lösung dieses Problems finden Sie unter: http://go.gfi.com/?pageid=ME_ExpImpBuild
Remote-Befehle funktionieren nicht.	Siehe: http://go.gfi.com/?pageid=ME_RemoteCommands
Die E-Mail-Bearbeitung ist sehr langsam.	Dies kann an DNS-Problemen im Netzwerk liegen. Falls DNS nicht korrekt arbeitet, verursachen die DNS-Suchen einiger Anti-Spam-Filter in GFI MailEssentials ein Timeout. Weitere Informationen finden Sie unter: http://go.gfi.com/?pageid=ME_ProcessingSlow
Bei Verwendung von Microsoft® Access sind ältere Daten in der Datenbank nicht verfügbar.	Wenn die Datenbank **reports.mdb** eine Größe von 1,7 GB überschreitet, wird sie automatisch in **reports_<Datum>.mdb** umbenannt, und eine neue Datenbank mit dem Namen **reports.mdb** wird erstellt. Weitere Informationen zur Lösung dieses Problems finden Sie unter: http://go.gfi.com/?pageid=ME_ReportDB
Die Quarantäneoberfläche zeigt Fehler D10 – **Es kann nicht auf die Datenbank des Quarantänespeichers zugegriffen werden. Verwenden Sie ein Datenbankreparatur-Tool (wie esentutl.exe), um die Datenbank zu reparieren.**	Weitere Informationen zum Reparieren der Quarantänespeicher-Datenbank mit esentutl.exe finden Sie unter http://go.gfi.com/?pageid=ME_esentutl.
Fehler beim Empfangen von E-Mails: **Textkörpertyp nicht von Remote-Host unterstützt**	Dieser Fehler tritt auf, wenn E-Mails vom IIS SMTP-Server zum Microsoft® Exchange-Server umgeleitet werden. Der Grund dafür ist, dass die Versionen 4.0, 5.0 und 5.5 von Microsoft® Exchange Server keine 8-Bit-MIME-Nachrichten verarbeiten können. Eine Anleitung zum Abschalten von 8BITMIME in Windows Server 2003 finden Sie unter: http://go.gfi.com/?pageid=ME_TurnOff8bitMIME.
Zulässige E-Mails werden in den Ordner **failedmails** verschoben.	**Ursache** Wenn GFI MailEssentials eingehende E-Mails nicht scannen kann, werden diese E-Mails nicht an den Empfänger zugestellt, da sie schädliche Inhalte aufweisen könnten. GFI MailEssentials verschiebt diese E-Mails in den folgenden Ordner: *<GFI MailEssentials Installationspfad>*\GFI\MailEssentials\EmailSecurity\failedmails\ **Lösung** Werden zulässige E-Mails in den failedmails-Ordner verschoben, können diese manuell erneut verarbeitet und somit zugestellt werden. Weitere Informationen finden Sie unter „Fehlgeschlagene E-Mails“ (Seite 259). Weitere Informationen zu fehlgeschlagenen E-Mails finden Sie unter: http://go.gfi.com/?pageid=ME_FailedMails
Muss ich ein Upgrade meines Lizenzschlüssels durchführen, wenn ich ein Upgrade auf eine neue Version vornehme?	Informationen zur Lizenzierung finden Sie hier: http://go.gfi.com/?pageid=ME_adminManualEN
Wo finde ich die Online-Version dieses Handbuchs?	Die Online-Version dieses Handbuchs ist hier verfügbar: http://go.gfi.com/?pageid=GFI_Manuals

12.3 Scan-Engines und Filter

Aufgetretenes Problem	Lösung
Spam wird an Benutzerpostfach zugestellt.	Gehen Sie nach der folgenden Checkliste vor, um das Problem zu lösen: 1. Stellen Sie sicher, dass das Scannen von E-Mails in GFI MailEssentials nicht deaktiviert ist. Weitere Informationen finden Sie unter „Deaktivieren der E-Mail-Verarbeitung“ (Seite 281). 2. Überprüfen Sie, ob alle erforderlichen Filter aktiviert sind. Weitere Informationen finden Sie unter „Anti-Spam-Filter“ (Seite 111). 3. Überprüfen Sie, ob die lokalen Domänen korrekt konfiguriert sind. Weitere Informationen finden Sie unter „Lokale Domänen“ (Seite 248). 4. Überprüfen Sie, ob E-Mails zu GFI MailEssentials geleitet werden bzw. ob GFI MailEssentials an den richtigen virtuellen IIS SMTP-Server gebunden ist. 5. Überprüfen Sie, ob der Speicherort '%TEMP%' (standardmäßig der Ordner ‘C:\Windows\Temp’) viele Dateien enthält. 6. Überprüfen Sie, ob die Anzahl der Benutzer, die GFI MailEssentials verwenden, die Anzahl der erworbenen Lizenzen übersteigt. 7. Überprüfen Sie, ob die Whitelist korrekt konfiguriert ist. Weitere Informationen finden Sie unter „Whitelist“ (Seite 142). 8. Überprüfen Sie, ob die Aktionen korrekt konfiguriert sind. Weitere Informationen finden Sie unter „Spam-Aktionen – Umgang mit Spam-E-Mails“ (Seite 150). 9. Überprüfen Sie, ob die Bayes'sche Analyse korrekt konfiguriert ist. Weitere Informationen finden Sie unter „Bayes'sche Analyse“ (Seite 140). Weitere Informationen zur Lösung dieses Problems finden Sie unter: http://go.gfi.com/?pageid=ME_SpamChecklist
Das Laden der Seiten für die E-Mail-Blocklist, die Whitelist oder die Inhaltsfilterung dauert sehr lang oder scheint nicht zu funktionieren.	Begrenzen Sie die Anzahl der Einträge in den Listen auf 10.000.
SpamRazer-Aktualisierungen werden nicht heruntergeladen.	1. Stellen Sie sicher, dass Ihr Lizenzschlüssel gültig ist. 2. Stellen Sie sicher, dass die erforderlichen Ports offen sind und Ihre Firewall Verbindungen vom GFI MailEssentials-Server erlaubt. Weitere Informationen finden Sie unter „Firewall-Port-Einstellungen“ (Seite 24). 3. Stellen Sie sicher, dass die Proxy-Server-Einstellungen (falls vorhanden) für die Verbindung mit dem Internet korrekt sind.
E-Mails werden nicht auf die Greylist gesetzt.	So prüfen Sie das Funktionieren der Greylist: **Schritt 1: Sicherstellen, dass die Greylist aktiviert ist** Stellen Sie in den Eigenschaften der Greylist sicher, dass die Greylist aktiviert ist. **Schritt 2: Verifizieren ausgeschlossenen Adressen** Stellen Sie im Bereich der IP- und E-Mail-Ausnahmen in den Greylist-Eigenschaften sicher, dass keine falschen Ausnahmen (wie *@*.com) enthalten sind. **Schritt 3: Stellen Sie mit esentutl.exe sicher, dass die Greylist-Datenbank korrekt funktioniert.** Weitere Informationen finden Sie unter: http://go.gfi.com/?pageid=ME_esentutl

Aufgetretenes Problem	Lösung
Sie empfangen Spam-E-Mails von Ihrer Domäne.	Einige Spam-E-Mails enthalten eine gefälschte SMTP FROM-E-Mail-Adresse mit der gleichen Domäne wie der Empfänger. Deshalb scheint es so, als würde die E-Mail von einem lokalen Benutzer kommen. 1. Aktivieren Sie im SpamRazer-Filter das Sender Policy Framework, um E-Mails von gefälschten Absendern zu blockieren. Weitere Informationen finden Sie unter „SpamRazer“ (Seite 112). 2. Erstellen Sie einen SPF-Eintrag für Ihre Domäne. Weitere Informationen finden Sie unter http://go.gfi.com/?pageid=ME_CreateSPFRecord. 3. Stellen Sie sicher, dass SpamRazer mit einer höheren Priorität als das Whitelist-Modul ausgeführt wird. Weitere Informationen finden Sie unter „Sortieren der Anti-Spam-Filter nach Priorität“ (Seite 153).
E-Mails von Absendern in der Whitelist werden blockiert.	1. E-Mails von Whitelist-Absendern können blockiert werden, wenn sie Inhalte oder Anhänge aufweisen, die Anti-Malware-Regeln verletzen, da diese eine höhere Priorität als die Whitelist haben. Vergewissern Sie sich, dass die blockierten E-Mails keine Anti-Malware-Regeln verletzen. 2. Stellen Sie die Filterprioritäten so ein, dass die Whitelist über allen Filtern steht, die die gewünschte E-Mail blockieren. Weitere Informationen finden Sie unter: http://go.gfi.com/?pageid=ME_BlockedWhitelistedSenders
Spam wird nicht an den Microsoft® Exchange-Unterordner oder den festgelegten Outlook-Unterordner in einer Microsoft® Exchange Server 2010-Umgebung zugestellt.	1. Überprüfen Sie, ob diese Funktion korrekt konfiguriert ist. Weitere Informationen finden Sie unter „Verschieben von Spam in einen Exchange 2010-Ordner“ (Seite 268). 2. Ausführliche Informationen zur Behebung dieses Problems finden Sie unter http://go.gfi.com/?pageid=ME_AutodiscoverIssues.

12.4 E-Mail-Verwaltung

Aufgetretenes Problem	Lösung
Ausgehenden Nachrichten wird kein Haftungsausschluss hinzugefügt.	Haftungsausschlüsse werden nur ausgehenden E-Mails von Domänen hinzugefügt, die von GFI MailEssentials geschützt werden. Haftungsausschlüsse werden in folgenden Fällen nicht hinzugefügt: » E-Mails werden von Domänen gesendet, die nicht in der Liste der lokalen Domänen festgelegt sind. » E-Mails werden an Domänen gesendet, die in der Liste der lokalen Domänen enthalten sind, und somit als interne E-Mails behandelt. Stellen Sie sicher, dass alle lokalen Domänen im Dialogfeld für eingehende E-Mail-Domänen angegeben sind. Weitere Informationen finden Sie unter „Lokale Domänen“ (Seite 248).
Einige Zeichen im Haftungsausschlusstext werden nicht korrekt angezeigt.	Konfigurieren Sie Microsoft® Outlook so, dass keine automatische Codierung verwendet wird und die Verwendung der richtigen Codierung durch GPO erzwungen wird. Weitere Informationen zur Lösung dieses Problems finden Sie unter: http://go.gfi.com/?pageid=ME_Outlook2003Encoding
E-Mails an den Listenserver werden in Nur Text konvertiert.	E-Mails an den Listenserver werden nur dann in Klartext konvertiert, wenn das Originalformat der E-Mails RTF ist. Senden Sie E-Mails im HTML-Format, um das Originalformat beizubehalten.
Interne Benutzer erhalten einen Unzustellbarkeitsbericht, wenn sie E-Mails an den Listenserver senden und GFI MailEssentials auf einem Gateway-Rechner installiert ist.	Informationen dazu, wie Sie die Listenserverfunktion verwenden, wenn GFI MailEssentials auf einem Gateway installiert ist, finden Sie hier: http://go.gfi.com/?pageid=ME_ListServerGateway
E-Mails von bestimmten Benutzern oder an bestimmte Benutzer werden nicht überwacht.	E-Mails vom oder an den GFI MailEssentials-Administrator und die E-Mail-Adresse, an die die überwachten E-Mails gesendet werden, werden von den E-Mail-Überwachungsregeln nicht überwacht. Die E-Mail-Überwachungsregeln gelten auch nicht für E-Mails zwischen internen Benutzern desselben Informationsspeichers.

12.5 GFI SkyNet

GFI pflegt ein umfangreiches Knowledge Base-Repository, in dem Lösungen für die häufigsten Probleme beschrieben sind. GFI SkyNet enthält immer die aktuelle Liste der Fragen, die an den technischen Support gerichtet wurden, sowie die neuesten Patches. Wenn die Informationen in dieser Anleitung nicht ausreichen, um Ihre Probleme zu lösen, schlagen Sie bitte unter GFI SkyNet nach: http://kb.gfi.com/.

12.6 Webforum

Über das GFI-Webforum erhalten Sie technischen Support von Benutzer zu Benutzer. Zum Webforum gelangen Sie über folgende URL-Adresse: http://forums.gfi.com/.

12.7 Technischen Support anfragen

Wenn Sie mit keiner der oben angegebenen Ressourcen Ihre Probleme beheben können, wenden Sie sich bitte an das technische Supportteam von GFI. Füllen Sie dazu ein Online-Support-Formular aus, oder rufen Sie an.

» **Online**: Füllen Sie das Anfrageformular für den Support aus, und befolgen Sie genau die Anweisungen auf dieser Seite, um Ihre Support-Anfrage unter folgendem Link zu übermitteln: http://support.gfi.com/supportrequestform.asp

» **Telefon**: Die korrekte Telefonnummer für den technischen Support Ihrer Region finden Sie unter: http://www.gfi.com/company/contact.htm.

> **HINWEIS**
>
> Halten Sie bitte Ihre Kundennummer bereit, wenn Sie sich an den technischen Support wenden. Ihre Kundennummer entspricht der Online-Kontonummer, die Sie bei der ersten Registrierung Ihrer Lizenzschlüssel im GFI-Kundenbereich unter folgendem Link erhalten haben: http://customers.gfi.com.

Für die Beantwortung Ihrer Anfrage benötigt GFI in Abhängigkeit von Ihrer Zeitzone maximal 24 Stunden.

12.8 Dokumentation

Wenn dieses Handbuch Ihren Erwartungen nicht entspricht oder Sie der Meinung sind, dass die Dokumentation verbessert werden kann, senden Sie uns bitte eine E-Mail an: documentation@gfi.com.

13 Anhang - Bayes'scher Filter

Der Bayes'sche Filter ist eine Anti-Spam-Technologie, die von GFI MailEssentials verwendet wird. Es handelt sich um eine adaptive Technik, die auf Algorithmen aus der Künstlichen Intelligenz basiert, um ein maximales Spektrum an Spam-Technologien abzuwehren.

In diesem Kapitel wird die Funktionsweise des Bayes'schen Filters detailliert erklärt, und Sie erfahren, wie der Filter konfiguriert und trainiert wird.

> **HINWEIS**
>
> 1. Der Bayes'sche Anti-Spam-Filter ist standardmäßig deaktiviert. Es wird dringend empfohlen, den Filter zu trainieren, bevor Sie ihn aktivieren.
>
> 2. GFI MailEssentials muss mindestens eine Woche lang ausgeführt werden, damit der Bayes'sche Filter seine optimale Leistung erreichen kann. Dies ist erforderlich, da der Bayes'sche Filter erst durch die Anpassung an Ihre E-Mail-Muster eine maximale Erkennungsquote erzielen kann.

Funktionsweise des Bayes'schen Spam-Filters

Die Bayes'sche Filtertechnologie basiert auf dem mathematischen Prinzip, dass die meisten Ereignisse voneinander abhängig sind und dass die Wahrscheinlichkeit eines zukünftigen Ereignisses aus vorherigen Ereigniseintritten abgeleitet werden kann.

> **HINWEIS**
>
> Weitere mathematische Hintergrundinformationen zur Bayes'schen Filtertechnologie finden Sie hier:
>
> http://go.gfi.com/?pageid=ME_BayesianParameterEstimation

Dieses Prinzip wurde von GFI MailEssentials adaptiert, um Spam-E-Mails zu identifizieren und klassifizieren. Bestimmte Begriffe oder Inhalte werden oft nur in Spam-Nachrichten verwendet und kommen in zulässigen E-Mails nicht vor. Daraus lässt sich schließen, dass es sich bei Nachrichten mit solchen Inhalten wahrscheinlich um Spam handelt.

Erstellen einer angepassten Bayes'schen Begriffsdatenbank

Bevor der Bayes'sche Filter verwendet werden kann, muss eine Datenbank mit Wörtern und Tokens (z. B. das $-Zeichen, IP-Adressen, Domänen usw.) erstellt werden. Diese können aus Spam-Beispielen und gültigen E-Mails (auch als 'Ham' bezeichnet) erfasst werden.

Danach wird jedem Wort oder Token ein Wahrscheinlichkeitswert zugewiesen. Dieser basiert auf Berechnungen, in die einfließt, wie oft das betreffende Wort in Spam-Nachrichten im Vergleich zu erwünschten Nachrichten vorkommt. Dazu werden ausgehende Benutzer-E-Mails und bekannte Spam-Nachrichten analysiert: Alle Wörter und Tokens in beiden E-Mail-Pools werden analysiert, um bestimmten Wörtern einen Wahrscheinlichkeitswert zuzuweisen, der sie als Spam-typisch klassifiziert.

Der Wahrscheinlichkeitswert wird wie im folgenden Beispiel berechnet:

Beim Wort 'Hypothek', das in 400 von 3.000 Spam-Mails und in 5 von 300 erwünschten E-Mails vorkommt, liegt die Spam-Wahrscheinlichkeit bei 0,8889 (d. h. [400/3000] / [5/300 + 400/3000]).

Erstellen einer benutzerdefinierten Ham-Datenbank

Die Analyse von Ham-E-Mails wird anhand der E-Mail-Korrespondenz des jeweiligen Unternehmens vorgenommen und gilt daher nur für dieses Unternehmen.

» **Beispiel:** Ein Finanzunternehmen verwendet das Wort ‘Hypothek’ sehr häufig, daher würde die Verwendung allgemein gültiger Anti-Spam-Regeln hier zu vielen falsch-positiven Ergebnissen führen. Nach einer anfänglichen Lernphase und Anpassung an die Unternehmenskorrespondenz berücksichtigt der Bayes'sche Filter jedoch die gültige ausgehende Post des Unternehmens (und erkennt dabei ‘Hypothek’ als häufig genutzten Begriff in ordnungsgemäßen E-Mails). Auf diese Weise wird eine sehr hohe Spam-Erkennungsrate bei minimaler Fehlalarmrate erzielt.

Erstellen der Bayes'schen Spam-Datenbank

Neben den Ham-E-Mails stützt sich der Bayes'sche Filter auf eine Datei mit Spam-Daten. Diese Spam-Datei muss eine große Menge bekannter Spam-Nachrichten enthalten. Zudem muss sie kontinuierlich von der Anti-Spam-Software mit den neuesten Spam-Nachrichten aktualisiert werden. Hierdurch wird sichergestellt, dass der Bayes’sche Filter auch sämtliche neuen Spam-Trends erkennt und eine hohe Erkennungsrate erzielt.

Wie erfolgt die Bayes'sche Filterung?

Sind die Datenbanken für Ham- und Spam-Nachrichten erstellt, kann der Spam-Wahrscheinlichkeitswert für die einzelnen Wörter berechnet werden, und der Filter ist einsatzbereit.

Trifft eine neue E-Mail ein, wird sie in ihre einzelnen Wörter aufgeschlüsselt, wobei die wichtigsten Wörter (die mit der größten Relevanz für die Klassifizierung von E-Mails als Spam) identifiziert werden. Unter Berücksichtigung dieser Wörter errechnet der Bayes'sche Filter die Wahrscheinlichkeit, ob eine neue Nachricht als Spam eingestuft werden muss. Ist die Wahrscheinlichkeit größer als ein bestimmter Schwellenwert, wird die Nachricht als Spam klassifiziert.

> **HINWEIS**
>
> Weitere Informationen zur Bayes'schen Filterung und ihren Vorteilen finden Sie unter:
>
> http://go.gfi.com/?pageid=ME_Bayesian

13.0.1 Trainieren des Bayes'schen Analysefilters

> **HINWEIS**
>
> Der Bayes'sche Analysefilter kann auch mithilfe von öffentlichen Ordnern trainiert werden. Weitere Informationen finden Sie unter „Konfigurieren des Bayes'schen Filters“ (Seite 140).

Es wird empfohlen, den Bayes'schen Analysefilter anhand der E-Mail-Korrespondenz des Unternehmens über einen gewissen Zeitraum zu trainieren. Es ist auch möglich, die Bayes'sche Analyse mit E-Mails zu trainieren, die vor der Installation von GFI MailEssentials gesendet und empfangen wurden. Dafür kann der Assistent für die Bayes'sche Analyse verwendet werden. Auf diese Weise kann die Bayes'sche Analyse sofort aktiviert werden.

Der Assistent analysiert folgende Quellen:

» Zulässige E-Mails (z. B. Postfachordner für gesendete Objekte)

» Spam-E-Mails (z. B. Postfachordner für Spam-E-Mails)

Schritt 1: Assistent für Bayes'sche Analyse installieren

Der Assistent für die Bayes'sche Analyse kann auf folgenden Computern installiert werden:

» Ein Rechner, der mit Microsoft® Exchange kommuniziert – um E-Mails in einem Postfach zu analysieren

» Ein Rechner, auf dem Microsoft Outlook installiert ist – um E-Mails in Microsoft Outlook zu analysieren

1. Kopieren Sie die Setup-Datei **bayesianwiz.exe** des Assistenten für die Bayes'sche Analyse auf den ausgewählten Rechner. Der Pfad zu dieser Datei lautet:

Installationspfad von GFI MailEssentials*AntiSpam\BSW*

2. Starten Sie **bayesianwiz.exe**, und klicken Sie im Willkommensbildschirm auf **Weiter**.

Wählen Sie den Installationsordner aus, und klicken Sie auf **Weiter**.

4. Klicken Sie auf **Weiter**, um die Installation zu starten.

5. Klicken Sie auf **Fertig stellen**, wenn die Installation abgeschlossen ist.

Schritt 2: Zulässige und Spam-E-Mails analysieren

So starten Sie die Analyse von E-Mails mithilfe des Assistenten für die Bayes'sche Analyse:

1. Starten Sie den Assistenten für die Bayes'sche Analyse unter **Start > Programme > GFI MailEssentials > GFI MailEssentials Assistent für Bayes'sche Analyse**.

2. Klicken Sie im Willkommensbildschirm auf **Weiter**.

3. Wählen Sie eine der beiden Möglichkeiten:

» Eine neue Bayes'sche Spam-Profil-Datei (.bsp) erstellen oder eine vorhandene aktualisieren. Legen Sie den Dateinamen und den Pfad fest, wo die Datei gespeichert werden soll.

» Das Bayes'sche Spam-Profil aktualisieren, das vom Bayes'schen Analysefilter direkt verwendet wird, wenn er auf demselben Rechner wie GFI MailEssentials installiert wird.

Klicken Sie auf **Weiter**, um fortzufahren.

4. Wählen Sie aus, wie der Assistent auf zulässige E-Mails zugreifen soll. Wählen Sie:

» **Microsoft Outlook-Profil verwenden, das auf diesem Computer konfiguriert ist** – Fragt E-Mails von einem Mail-Ordner in Microsoft Outlook ab. Microsoft Outlook muss ausgeführt werden, um diese Option zu verwenden.

» **Mit Microsoft® Exchange Server-Postfachspeicher verbinden** – Fragt E-Mails von einem Microsoft® Exchange-Postfach ab. Geben Sie die Anmeldedaten im nächsten Bildschirm an.

» **Zulässige E-Mails (Ham) nicht im Bayes'schen Spam-Profil aktualisieren** – Die Abfrage von zulässigen E-Mails wird übersprungen. Fahren Sie mit Schritt 6 fort.

Klicken Sie zum Fortfahren auf **Weiter**.

5. Nachdem der Assistent eine Verbindung zur Quelle hergestellt hat, wählen Sie den Ordner aus, der die Liste der zulässigen E-Mails enthält (z. B. Ordner für gesendete Objekte). Klicken Sie anschließend auf **Weiter**.

6. Wählen Sie aus, wie der Assistent auf die Quelle für Spam-E-Mails zugreifen soll. Wählen Sie:

» **Aktuelles Spam-Profil von der GFI-Website herunterladen** – Lädt eine Spam-Profildatei herunter, die regelmäßig durch das Sammeln von Mails von führenden Spam-Archivseiten aktualisiert wird. Es ist eine Internetverbindung erforderlich.

» **Microsoft Outlook-Profil verwenden, das auf diesem Computer konfiguriert ist** – Fragt Spam-E-Mails von einem Mail-Ordner von Microsoft Outlook ab. Microsoft Outlook muss ausgeführt werden, um diese Option zu verwenden.

» **Mit Microsoft® Exchange Server-Postfachspeicher verbinden** – Fragt Spam-E-Mails von einem Microsoft® Exchange-Postfach ab. Geben Sie die Anmeldedaten im nächsten Bildschirm an.

» **Spam im Bayes'schen Spam-Profil nicht aktualisieren** – Überspringt die Abfrage von Spam-E-Mails. Fahren Sie mit Schritt 8 fort.

Klicken Sie zum Fortfahren auf **Weiter**.

7. Wählen Sie, nachdem sich der Assistent mit der Quelle verbunden hat, den Ordner aus, der die Liste der Spam-E-Mails enthält. Klicken Sie anschließend auf **Weiter**.

8. Klicken Sie auf **Weiter**, um die Abfrage der festgelegten Quellen zu starten. Dieser Vorgang kann einige Minuten dauern.

9. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Schritt 3: Bayes'sches Spam-Profil importieren

Wenn der Assistent nicht auf dem Server von GFI MailEssentials läuft, importieren Sie die Bayes'sche Spam-Profil-Datei (.bsp) in GFI MailEssentials.

1. Verschieben Sie die Datei in den Ordner **Data** im Installationspfad von GFI MailEssentials.

2. Starten Sie die **GFI MailEssentials AS-Scan-Engine** und den **GFI MailEssentials Legacy Attendant**-Dienst neu.

14 Glossar

A

Active Directory
Eine Technologie, die verschiedene Netzwerkdienste bereitstellt (darunter LDAP-Verzeichnisdienste).

AD
Siehe Active Directory

Anti-Virus-Software
Software, die Malware wie Trojaner in E-Mails, Dateien und Anwendungen erkennt.

Automatische Antwort
Eine automatische E-Mail-Antwort für eingehende E-Mails.

B

Bayes'sche Filterung
Eine Anti-Spam-Technik, bei der ein statistischer Wahrscheinlichkeitsindex basierend auf einer Benutzeranalyse zur Erkennung von Spam verwendet wird.

BITS
Siehe intelligenter Hintergrundübertragungsdienst (Background Intelligent Transfer Service)

Blocklist
Eine Liste von E-Mail-Adressen oder Domänen, von denen Benutzer keine E-Mails empfangen sollen.

Botnet
Ein Netzwerk aus infizierten Computern, die autonom ausgeführt und von einem Hacker kontrolliert werden.

C

CIDR
Siehe klassenloses domänenübergreifendes Routing (Classless Inter-Domain Routing)

D

Dekomprimierungs-Engine
Ein Scan-Modul, das Archive (z. B. ZIP- und RAR-Dateien) dekomprimiert und analysiert, die an E-Mails angehängt sind.

Demilitarized Zone
Ein Netzwerkbereich mit Internetzugriff, der nicht Bestandteil des internen Netzwerks ist. Der Bereich fungiert in der Regel als Gateway zwischen internen Netzwerken und dem Internet.

Directory Harvesting

E-Mail-Angriffe, bei denen bekannte E-Mail-Adressen als Vorlage zum Erstellen anderer E-Mail-Adressen verwendet werden.

DMZ

Siehe Demilitarized Zone

DNS

Siehe Domain Name System

DNS MX

Siehe Mail Exchange

Domain Name System

Eine in TCP/IP-basierten Netzwerken verwendete Datenbank, mit der sich Hostnamen in IP-Adressen übersetzen und andere Domänen-bezogene Informationen bereitstellen lassen.

E

E-Mail-Header

Informationen, die dem E-Mail-Text(feld) in einer Nachricht vorausgehen. Hierzu gehören Absender, Empfänger, Betreff, Sende- und Empfangszeitstempel usw.

E-Mail-Überwachungsregeln

Regeln, die die Replikation von E-Mails zwischen E-Mail-Adressen ermöglichen.

Exploit

Eine Angriffsmethode, die bekannte Schwachstellen in Anwendungen oder Betriebssystemen ausnutzt, um die Sicherheit eines Systems zu gefährden.

F

Falsch-negative Ergebnisse

Spam-E-Mails, die nicht als Spam erkannt werden.

Falsch-positive Ergebnisse

Zulässige E-Mails, die fälschlicherweise als Spam erkannt werden.

G

Gateway

Der Computer (Server) in einem LAN, der direkt mit einem externen Netzwerk verbunden ist. In GFI MailSecurity bezieht sich Gateway auf die Mailserver in einem Unternehmen, die E-Mails von externen Domänen als Erste empfangen.

Greylist-Filterung

Ein Anti-Spam-Filter, der E-Mails von Spammern blockiert, die keine Nachricht zurückschicken, wenn eine Versuchsnachricht empfangen wurde.

H

Haftungsausschluss
Eine Erklärung, die den Umfang der Rechte und Pflichten für E-Mail-Empfänger definiert oder begrenzt.

Ham
Zulässige E-Mails

HTML-Bereinigung
Ein Filtermodul in GFI MailSecurity, das HTML-Skript-Code scannt und aus E-Mails entfernt.

HTTP
Hypertext Transfer Protocol – Ein Protokoll zur Übertragung von Hypertextdaten zwischen Servern und Internetbrowsern.

I

IIS
Siehe Internetinformationsdienste

IMAP
Siehe Internet Message Access Protocol

Intelligenter Hintergrundübertragungsdienst
Eine Komponente von Microsoft Windows-Betriebssystemen, die nicht genutzte Netzwerkbandbreite für die Übertragung von Dateien zwischen Systemen verwendet.

Internet Message Access Protocol
Eines der beiden häufigsten Standardprotokolle im Internet für das Abrufen von E-Mails. Das andere ist POP3.

Internetinformationsdienste
Eine Gruppe an internetbasierten Diensten, die die Microsoft Corporation für Internetserver entwickelt hat.

K

Klassenloses domänenübergreifendes Routing
Eine Notation für IP-Adressen zum Festlegen eines IP-Adressbereichs.

L

LDAP
Siehe Lightweight Directory Access Protocol

Lightweight Directory Access Protocol
Ein Anwendungsprotokoll zum Abfragen und Ändern von Verzeichnisdiensten über TCP/IP.

Listenserver

Ein Server, der E-Mails an Diskussionslisten und Newsletter-Listen verteilt und Abonnementanfragen verwaltet.

M

Mail Exchange

Der DNS-Eintrag für die Identifizierung der IP-Adressen der Domänen-Mailserver.

Malware

Alle Arten von Schadsoftware, die die Computersicherheit gefährden und für gewöhnlich mit böswilligen Methoden verbreitet werden.

MAPI

Siehe Message Application Programming Interface

MDAC

Siehe Microsoft Data Access Components

Messaging Application Programming Interface

Eine Messaging-Architektur und eine auf einem Komponentenobjektmodell basierte Schnittstelle für die Programmierung von Anwendungen (API) für Microsoft Exchange.

Microsoft Data Access Components

Eine Microsoft-Technologie, die eine einheitliche und konsistente Möglichkeiten zur Entwicklung von Software bietet, die auf nahezu jeden Datenspeicher zugreifen kann.

Microsoft Message Queuing-Dienste

Eine Nachrichtenwarteschlangen-Implementierung für Windows Server-Betriebssysteme.

MIME

Siehe Multipurpose Internet Mail Extensions

MSMQ

Siehe Microsoft Message Queuing-Dienste

Multipurpose Internet Mail Extensions

Ein Standard, der das E-Mail-Format erweitert, um Nicht-ASCII-Zeichen in Texten und Kopfzeilen, Nicht-Text-Anhänge und Textnachrichten mit mehreren Teilen zu unterstützen.

N

NDR

Siehe Unzustellbarkeitsbericht (Non Delivery Report)

Ö

Öffentlicher Ordner

Ein gemeinsamer Ordner, über den Microsoft Exchange-Benutzer Informationen austauschen können.

P

Perimeter-Server/-Gateway

Der Host in einem LAN, der direkt mit einem externen Netzwerk verbunden ist. In GFI MailEssentials bezieht sich Perimeter-Gateway auf die Mailserver in einem Unternehmen, die E-Mails von externen Domänen als Erste empfangen.

PGP-Verschlüsselung

Ein Kryptosystem mit öffentlichen Schlüsseln, das häufig zur Verschlüsselung von E-Mails verwendet wird.

Phishing

Das Erfassen sensibler persönlicher Daten mit betrügerischer Absicht, meist mithilfe von gefälschten Kommunikationsmitteln.

POP2Exchange

Ein System, das E-Mails von POP3-Postfächern sammelt und an den Mailserver weiterleitet.

POP3

Siehe Post Office Protocol 3

Post Office Protocol 3

Ein Client/Server-Protokoll zum Speichern von E-Mails, mit dem Clients jederzeit eine Verbindung zum POP3-Server aufbauen und E-Mails abrufen können. Der Mail-Client baut hierbei eine TCP/IP-Verbindung mit dem Server auf, und durch den Austausch mehrerer Befehle können E-Mails dann vom Benutzer gelesen werden.

Q

Quarantäne

Eine E-Mail-Datenbank zur Speicherung von erkannten Spam- oder Malware-E-Mails in einer kontrollierten Umgebung. E-Mails in der Quarantäne sind keine Bedrohung für die Netzwerkumgebung.

Quarantänespeicher

Ein zentraler Speicher in GFI MailSecurity, in dem blockierte E-Mails aufbewahrt werden, bis sie von einem Administrator überprüft werden.

R

RBL

Siehe Realtime Blocklist

Realtime Blocklist

Eine Online-Datenbank mit Spam-IP-Adressen. Eingehende E-Mails werden mit diesen Listen verglichen, um festzustellen, ob sie von blockierten Benutzern stammen.

Rekursive Archive

Archive, die mehrere Ebenen von Unterarchiven (Archive innerhalb von Archiven) enthalten. Sie werden auch als verschachtelte Archive bezeichnet.

Remote-Befehle

Anweisungen, die die Ausführung von Aufgaben über Fernzugriff ermöglichen.

RSS-Feeds

Ein Protokoll, das von Websites zur Verteilung von häufig aktualisierten Inhalten (Feeds, z. B. Nachrichten) an die Abonnenten verwendet wird.

S

Secure Sockets Layer

Ein Protokoll, das die integrale und sichere Kommunikation zwischen Netzwerken sicherstellt.

Simple Mail Transport Protocol

Ein Internetstandard für die Übertragung von E-Mails über IP-Netzwerke.

SMTP

Siehe „Simple Mail Transport Protocol“

Spam-Aktionen

Aktionen, die für erhaltene Spam-E-Mails ausgeführt werden, z. B. Löschen der E-Mail oder Verschieben in den Junk-Mail-Ordner.

SSL

Siehe „Secure Sockets Layer“

T

Trojaner

Schadsoftware, die einen Computer gefährdet, indem sie sich als legitime Software tarnt.

U

Unzustellbarkeitsbericht

Eine automatisierte E-Mail, die bei einem E-Mail-Zustellungsproblem an den Absender gesendet wird.

V

Virenscan-Engine

Eine Virenerkennungstechnologie innerhalb einer Virenschutzsoftware, die für die tatsächliche Erkennung von Viren zuständig ist.

W

WebDAV

Eine Erweiterung von HTTP, mit der Benutzer Dateien remote und interaktiv verwalten können. Sie wird zur Verwaltung von E-Mails im Postfach und im öffentlichen Ordner in Microsoft Exchange verwendet.

Whitelist

Eine Liste von E-Mail-Adressen und Domänen, deren E-Mails immer als zulässig empfangen werden.

Z

Zombie

Ein infizierter Computer, der mittels Malware Teil eines Botnets wird.

15 Index

A

Active Directory 16, 19, 24, 32, 41, 49, 111, 117, 169, 176, 227, 233, 249, 251, 269, 277, 280

Aktualisierungen 24, 48, 59-60, 73, 76, 81, 85, 90, 95, 102, 105, 112, 115-116, 141, 247, 251, 275, 290

Anhangsfilterung 15, 183, 187, 207, 246, 249

Anti-Spam 10, 14, 16, 19-20, 24, 31, 38, 46, 48, 55, 63, 65, 111-112, 115, 117, 120, 122-123, 125, 127, 129, 131-132, 134, 138, 140, 142, 146, 148, 150, 153-154, 156, 158-161, 164, 167, 174-175, 178, 214, 218, 246, 268-269, 290, 294

Anti-Virus-Lösungen 15, 21, 24, 48, 59, 73, 75, 79, 84, 88, 93, 102, 105, 205, 219

Assistent 295

Automatische Antworten 11, 14, 236

B

Bayes'sche Analyse 16, 24, 112, 140, 246, 291

C

Cluster 23, 25, 29, 72

D

Dashboard 53-54, 57, 59-61, 289

Datenbank 16, 34-35, 53, 60-61, 68, 99, 111, 115, 120, 123, 132, 141, 161, 240, 249, 276, 290-291, 294

DEP 49

Directory Harvesting 14, 16, 49, 111, 117, 155, 246, 277, 280

DMZ 18, 25, 41, 176, 229

DNS-Server 28, 32, 125, 136

Domäne 31-32, 41, 49, 111, 117, 126, 130-131, 136, 142, 168, 175, 240, 249, 269, 289

E

E-Mail-Blocklist 16, 111, 120, 123, 161, 166, 179, 246, 291

E-Mail-Richtung 63, 65, 68, 108

E-Mail-Überwachung 11, 14-15, 243

F

Filterung ausgehender E-Mails 14

Filterung eingehender E-Mails 14

Firewall 18, 24, 40, 119, 229, 291

G

Gateway 18, 22-23, 25, 32, 40, 74, 78, 83, 87, 92, 128, 212, 219, 259, 289, 292

Greylist 16, 49, 111, 132, 155, 246, 291

H

Haftungsausschlüsse 11, 232, 292

Header-Prüfung 16, 112, 134

Hub-Transport 12, 17, 25, 96

I

IIS 19-20, 22, 25, 29, 33, 40, 132, 230, 248, 250-251, 254, 269, 277, 279, 289, 291

IMAP 36, 175, 289

Interne E-Mail-Adresse 28, 72

Internet 14, 32, 44, 125, 155, 165, 230, 246, 270, 291

IP 16, 26, 32, 43, 71, 108, 111, 124-125, 128, 131-132, 136, 146, 166, 229, 247, 262, 291

IP-Blocklist 16, 111, 123, 246

IP-DNS-Blocklist 16, 24, 111, 125, 153, 246

ISP 266

K

Kaspersky 15, 49, 73, 82

L

LDAP-Suche 119, 229

Leistung 27, 49, 145, 284, 294

Lizenzierung 249-250, 290

Lotus Domino 17, 24-25, 28, 31, 35, 174

Lotus Notes 28, 35

M

MAPI 175, 266

Microsoft Exchange 25, 152, 268

MSMQ 22

N

Nach der Installation 289

NET Framework 166

Neue Absender 14, 17, 112, 147, 153, 246

Newsletter 168, 179, 238, 241

P

Perimeter-Server 18, 25, 45, 109, 132, 277, 280

Phishing 16, 24, 48, 111, 115, 246, 267

POP2Exchange 11, 30, 53-54, 61, 262, 277, 279

POP3 28, 262, 289

Q

Quarantäne 10, 12, 15, 42, 46, 51, 58, 60, 75, 80, 84, 89, 94, 99, 104, 151, 184, 191, 197, 202, 208, 214, 217, 221, 254, 287

R

Remote-Befehle 15, 161, 290

RSS-Feeds 42, 221, 252, 257

S

Sender Policy Framework 16, 111-112, 128, 292

SMTP-Server 24-25, 42, 45, 125, 129, 131-132, 250

Spam-Aktionen 150, 276, 280

SpamRazer 16, 24, 111-112, 150, 246, 291

Stichwortprüfung 16, 112, 137, 161

U

Upgrade 10, 39, 47, 290

URI-DNS-Blocklist 16, 24, 111, 127, 246

V

VIPRE Email Security for Exchange 39

Virtuelles Verzeichnis 254, 270

W

WebDAV 175

Whitelist 15, 17, 108, 112-113, 123, 128, 131, 134, 136, 142, 146, 153, 161, 166, 174, 178, 246, 291

Z

Zulässige E-Mails 17, 49, 112, 119, 142, 178, 224, 290, 295

USA, KANADA UND ZENTRAL- SOWIE SÜDAMERIKA

4309 Emperor Blvd, Suite 400, Durham, NC 27703, USA

Telefon: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

GROSSBRITANNIEN UND IRLAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK

Telefon: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPA, MITTLERER OSTEN UND AFRIKA

GFI House, Territorials Street, Mriehel BKR 3000, Malta

Telefon: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIEN UND NEUSEELAND

83 King William Road, Unley 5061, South Australia

Telefon: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com